

Section 4: Legal foundations

This section provides detailed analyses by the project's partners of the eight legal foundations associated with overcoming barriers to eGovernment identified in Section 2. These were selected after a careful review of the relevant literature and by drawing on the knowledge of the legal partners and other experts involved in the project. The relevant expertise gained from previous experience, studies and research by the legal partners of the project's consortium allowed them to foresee that certain legal questions or legal areas could be problematic when considering eGovernment developments. After further discussion within the project and with other experts, eight main legal areas were identified. The selection criteria used to develop this list related to the likely extent of the impact of a legal issue on eGovernment.

The papers have been written by:

Dr. C Cuijpers and Dr. J. Nouwt, Tilburg Institute for Law, Technology, and Society (TILT), University of Tilburg, Netherlands: Authentication and Identification; Intellectual Property Rights; and Liability.

C. Dos Santos and Professor Cécile de Terwangne, CRID (Centre de Recherches Informatique et Droit), University of Namur, Belgium: Privacy and Data Protection; Public Administration Transparency; and Re-use of Public Sector Information

Dr Julián Valero Torrijos, University of Murcia, Spain: Administrative Law; Relationships between Public Administrations, Citizens and other ICT actors.

For each legal area, the following methodology was applied.

- The first step was to explain why the selected issues are or may become barriers to eGovernment.
- The second step was to explore the proposed solutions for each specific topic at the European Level and observe whether or not a framework is provided (e.g. a Directive, Recommendation, hard law, 'soft law'², etc.).
- Further analysis consisted of investigating whether the legal framework existing at the European level has solved problems and allows harmonious development of eGovernment, or whether barriers still remain. Many EC Directives relating to eGovernment include were examined (see References for a full list).
- The final activity, consisted of analysing whether an intervention at EU level is required, the reason why there is a need to intervene (or not) and the kind of intervention required. This is a key focus of the solutions report (deliverable 3).

² The term 'soft law' refers to quasi-legal instruments which do not have any binding force, or whose binding force is somewhat weaker than the binding force of traditional law, often referred to as 'hard law'. It initially appeared in the area of international law, but more recently it has been transferred to other branches of law. (Definition based on Wikipedia at: http://en.wikipedia.org/wiki/Soft_law)

Paper 1: Administrative Law and eGovernment

Dr Julián Valero Torrijos

University of Murcia, Spain

1. Description of this legal area

In most European states, public administrations are essentially governed by a specific regulation (called 'Administrative Law') that is different from those which govern the relationships between individuals. However, this is not applicable in such an intensive way in those countries, such as the UK, that are influenced by the legal Anglo-Saxon model of public administration which is ruled mainly by common law.

Administrative Law is characterized by the assignment of significant powers to public bodies and the recognition of relevant formal guarantees for citizens, based typically on a correct observance by public administrations of a legally predetermined sequence of steps. One of the main goals of Administrative Law is to ensure that administrative decisions must be adopted through the appropriate procedure: those that have been passed without respecting this formal requirement can be considered invalid. This is probably the most representative characteristic of Administrative Law, since it is an essential tool in controlling the correct formation of administrative decisions, both in terms of legality and opportunity.

As a general and complete vision of Administrative Law can not be offered for all the European countries, a special effort in order to understand the conception of each legal system—and particularly in the field of Administrative Law—must be done in order to advance in the European construction (Fromont, 2006) and, therefore, to overcome legal obstacles for eGovernment at the European level. As it has been highlighted (Fromont, 2006), in those countries of Roman legal tradition Administrative Law can be viewed as the specific legal framework for Public Administrations that does not comprise those rules that govern the activity of private individuals. Some examples can be given in order to assess the relevance of this regulation as a potential legal obstacle for eGovernment: according to these rules, administrative decisions can only be adopted by the competent authority—can a machine be considered as a public authority?—with a strict respect of the legally established procedure, which includes the obligation for the citizens to hand in all the required documents that sometimes must have a concrete format—is this compatible with the speed and flexibility offered by electronic means—and, as a consequence, if those requirements are not respected, administrative decisions may not be valid.

Therefore, if the rules specified in Administrative Law are made too rigid to accommodate the changes made possible by the use of ICTs, they could become obstacles to the effective implementation of eGovernment and erode confidence in it among citizens. On the other hand, if legal adaptations to accommodate eGovernment are limited to the general regulation of private individuals and do not affect Administrative Law, the lack of legal security regarding the use of ICT in administrative activities could become a major barrier to the modernization of public administration.

2. How is the area of Administrative Law related to barriers to eGovernment?

Generally, initiatives promoted by EU Member States to develop the use of ICT in the public sector have involved an intensive effort aimed at trying to overcome potential problems arising from the need to adapt the legal framework of their public administrations to the new challenges and problems. However, relevant essential reforms are still necessary in many cases in order to overcome some of the barriers imposed by the existence of specific Administrative Law regulations.

For instance, when 'traditional' Administrative Law rules are not adapted sufficiently to specific requirements related to ICT capabilities, a serious obstacle to the implementation of electronic public services may be created. Moreover, much new ICT-related legislation has been passed recently by Member States as a necessary adaptation to relevant European Directives, especially those related to digital signatures (Directive 1999/93/EC), eCommerce (Directive 2000/31/EC) and personal data protection (Directive 2002/58/EC). One of the main legal requirements in these fields is to fit modern regulation to the important singularities of Administrative Law and traditions in each Member State particularly in relation to the European perspective, which typically cannot take account of the concrete circumstances of each national legal public administration framework.

Therefore, an inadequate or non-existent adaptation of Administrative Law to the requirements of technology may involve a lower level of guarantee for private individuals and companies, which could threaten their essential role as users of electronic public services. As a result, eGovernment initiatives may lose their confidence. This would pose a very serious problem as the validity of administrative acts and respect for the rights of citizens may be damaged, making the modernization process involving eGovernment much more difficult.

3. What is the European context for this area, including legislation, policy statements and institutional arrangements relevant to this topic?

Many Member States have not taken sufficient account of the existence of a specific legal framework for public administration when implementing reforms promoted by the EU in the field of ICT, such as the Directives on data protection, digital signature and eCommerce. One reason for this is the absence in this area of a general competence reserved to the EU. Another is the intensive influence in some states of the legal Anglo-Saxon model of public administration based on common law. As a consequence, the implementation of these Directives by many of the Member States belonging to the 'continental model' of public administration based on Administrative Law have created some national rules that are not sufficiently adapted to the specific requirements of public administration regulation. Underestimating the particular needs of public administration activities can be considered to be a serious potential barrier to eGovernment since it can result in a risk of invalidating certain administrative decisions. This indicates why not all the legal solutions that have been applicable to eCommerce services can be automatically put into practice in the field of eGovernment.

These reasons may also explain why no direct references to Administrative Law have been found in the numerous documents on eGovernment analysed, most of them obtained from official EU websites. Consequently, we must focus our attention on the legal initiatives carried out by Member States. Some have passed overall eGovernment legislation in addition to the EU's general legal framework on ICT matters (e.g. eCommerce, digital signature and data protection). As shown at the website³ of the European Commission's IDABC programme to promote eGovernment in Europe, only Austria, the Czech Republic, Finland, Italy, Latvia, Slovakia and, recently, France have adopted this approach. Several other states (e.g. Slovenia and Spain) are in the process of preparing their eGovernment laws, which are due to be passed shortly. Analysis of these regulations is important to discovering whether they have overcome the existing barriers to eGovernment posed by Administrative Law or, on the contrary, have led to the appearance of new obstacles.

Certain European initiatives have had a direct impact on the field of Administrative Law since the existence of a specific – and singular – framework for public administration is closely related to some of the principles of the European common market. Specifically, particular requirements may not only hinder the effectiveness of an administrative activity but could also become a serious barrier for the competitiveness of the EU economy and European companies. Thus, any project for the technological modernization of public administration must take into account the ways electronic services provide a unique chance of simplifying administrative procedures, especially in terms of both data input by

³ <http://europa.eu.int/idabc/en/chapter/383>

users and the documentation to be provided⁴. Here, the *French eGovernment Strategic Plan*⁵ offers a relevant example as one of its main aims is to promote the evolution of law aimed at removing regulatory obstacles to the development of eGovernment and establishing an overall coherent legal framework that permits the development of eGovernment services. This includes the introduction of a new Bill on administration simplification to be presented to the Parliament by the Minister in charge of State Reform, which will contain an item on eGovernment. An Ordinance on electronic interactions between public services users and administrative authorities and between Administrations was adopted on 8 December 2005⁶ on the basis of the Legal Simplification Law of 9 December 2004 and is being processed as an Act at the National Parliament.

Finally, the consolidation of pan-European electronic services can also cause barriers at the national level since, although Administrative Law mostly remains a national prerogative, it has a major impact on eGovernment at the European level because those services are usually based on the activities – and therefore their legal limitations – of national, regional and local public administrations and their information systems. Underestimating, or not accounting for, different models of legal frameworks for public administrations can therefore be considered a serious potential barrier for the actual take-up and future expansion of pan-European eGovernment services.

4. What is the relationship of Administrative Law to the seven barrier categories and associated research questions?

4.1 Leadership failures (significant)

One of the main causes of the lack of adaptation of administrative legal frameworks to the requirements of ICT is the lack of effective leadership in ensuring special account is taken of eGovernment perspectives, particularly in relation to legal dimensions.

4.2 Financial inhibitors (significant)

The existence of a specific legal framework for public administrations could demand certain adaptations of the electronic means to deliver them that require a higher investment in developing, implementing and delivering eGovernment services. This inconvenience can frequently be removed with minor modifications of the present regulation to fit with the requirements of electronic technologies. Moreover, sometimes a *modern* interpretation of the *old* provisions which bears in mind the specific characteristics of ICT can be enough to solve that problem.

4.3 Digital Divides (significant)

Although the difficulties of certain groups in accessing eGovernment services are mainly produced by economic, cultural or technological circumstances that are not related to the regulation of the activity of public administrations, these issues may also be connected to the existence of an inappropriate legal framework for public administrations. This is particularly evident when old (non- adapted to ICT) or inappropriate regulations and requirements make it too difficult for an average citizen to access eGovernment services.

⁴ A Danish Commerce and Companies Agency (2005) report has noted that most of the hindrances to eGovernment introduced by the analysed laws were formal requirements.

⁵ <http://ec.europa.eu/idabc/en/document/4701/5679>

⁶ Ordinance 2005-1516, available at:

<http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0500286R>

From a different perspective, a wider access to digital networks could be promoted in some cases by public authorities if there were not relevant obstacles posed by Competition Law which cannot be identified directly with the requirements of Administrative Law. For example, this could involve subsidizing high-speed access to the Internet in rural zones as an essential requirement to promote the use of eGovernment services in those zones, which are usually located far from the main administrative offices.

4.4 Poor coordination (significant)

Technological adaptation of Administrative Law usually requires an effective coordination among all public administrations concerned, especially when national authorities have the competence to promote general modifications in this field which must be respected at regional and local levels.

From the European perspective, the lack of a general competence to approve regulations regarding public administrations is a relevant inconvenience that may also appear at the national level. Another potential legal obstacle to developing networked services can appear if, for political reasons, national authorities sometimes do not exercise their powers to establish more uniformity in relevant regional and local regulations. The constitutional autonomy of regions and local bodies could also become an obstacle. This can constrain certain administrative and organizational decisions designed to promote the use of electronic means, such as approaches based on a wide understanding of a citizen's right to use ICT to contact relevant authorities.

Some problems that were previously perceived primarily as being at the international level must also be considered as national scenarios, since the divergence of regional and local administrative regulations may become a serious obstacle to exchanging information in an effective way. Sometimes this situation demands general measures that must be adopted by national authorities, who may not have a clear competence for this purpose or may not want to exercise an existing competence to impose legal solutions that are the responsibility of regional and local powers.

The provision of eGovernment services to citizens and companies established in other Member States is much facilitated when there is a uniformed legal framework across Europe. Although some Directives and other European regulations have already sought to establish a minimum level of harmonization in some essential fields, such as data protection, public procurement and digital signatures, there are still some relevant divergences – not only in the specific regulation of each country but also in the interpretation and implementation of the European rules. This is illustrated by the way problems can be posed by the availability of certification service providers established in a different European country to the one where the public administration that offers the services is located, such as difficulties in validating the status of the certificates. Other inconveniences may also appear when eGovernment services are provided to other public authorities, particularly in the field of data protection where the diversity within national regulations may make it difficult to exchange information between authorities in different Member States.

4.5 Workplace and organizational flexibility (very significant)

One of the most important challenges to introducing eGovernment services is applying the technology's potential strengths in an effective way to help modernize and improve administrative activity. This opportunity will not be realized if traditional legal obstacles remain unreformed, particularly when the necessary simplification of administrative procedures is not undertaken and digital information is used instead of traditional paper-based documents in a manner that builds on the distinctive characteristics and advantages of ICT capabilities. A number of clear examples of traditional obstacles that should be

overcome are provided in Section 5.1.5, such as constraints imposed by the requirements of administrative procedures.

4.6 Lack of trust (significant)

The lack of adequate adaptation of traditional regulations based on personal and direct contact between citizens and public bodies may hinder the technological innovations offered by eGovernment to improve the quality of public services, particularly if citizens and companies are concerned that eGovernment provides a lower degree of legal security (e.g. through the automation of decisions and the nature of constraints imposed by the demands of formal administrative procedures).

One of the main problems in providing eGovernment services across Europe is that sometimes it is essential to prove certain facts or circumstances through documents drawn up by a public authority from another Member State. These could be subject to different formal and substantive requirements than those fixed by the regulation of the country in which the service is demanded. Since there are no overall EU criteria to solve this kind of cross-national problem, general rules should be adopted to clarify which regulation has to be applied when there is no clear and specific solution. A greater effort should also be made to harmonize the elements of public documents across Europe and to substitute paper-based documents by online exchanges of information where appropriate.

From a national perspective, there should be legal guarantee that it is not compulsory to present paper-based versions of those documents that are already in the possession of the public administration offering the electronic service. In order to simplify the procedure, and not force users to act as intermediaries between public administrations, public bodies could also ask for the authorization of citizens and companies through electronic means to facilitate the exchange of necessary information to exercise their competences.

A similar problem also appears when technological regulations do not bear in mind the singularities of administrative activity from a legal point of view, as occurs in the field of data protection, certificate service providing or eCommerce. Regulating the activities of public administrations mostly remain a prerogative of Member States as there is no general competence for this reserved to the EU, although there are some European regulations with a direct influence in this sector (e.g. public procurement of environmental protection services and technologies). In addition, ICT-related Directives with specific rules for public bodies do not usually impose a strong degree of uniformity. On the contrary, when Directives like 2000/31/EC on eCommerce keep silence about their application to public administration, a serious risk of uncertainty arises from the legal perspective. Therefore, it would be preferable to set a minimum specific provision for public bodies, which may be developed – or left at the minimum level – by each Member State, according to its own legal singularities and traditions.

A general requirement for the validity of administrative acts and decisions must be their adoption by the competent authority relevant to the field concerned. This requirement may not be respected when putting into action eGovernment services, since some decisions need to be made directly by a computer in order to achieve a higher efficiency. Many administrative regulations have been conceived and formulated for implementation through paper-based processes and personal relationships, which often mean they cannot be interpreted directly for application in an ICT-enabled environment. It is therefore likely that many traditional administrative regulations need to be adapted to avoid the negative consequences of a judicial review that may consider a public decision to be invalid if it does not offer a comparable level of guarantee with those adopted through traditional means.

Moreover, in certain cases more modern regulations – such as ICT-related Directives and national laws on digital signatures – may also not be suitable from this perspective. For example, it may be interpreted as an obstacle if the use of digital certificates has been

expressly established only for natural persons but not for computers and automated processes. A clearer regulation regarding this potential barrier should therefore aim to avoid offering such a condition, as it could hinder one of the main legal requirements for eGovernment services: the authentication and integrity of ICT systems and digital documents.

4.7 Poor technical design (not significant)

Some Member States have established legal obligations for public administrations to ensure access to eGovernment services is offered in good conditions from the perspective of technical design, particularly for websites and access to administrative information. Nevertheless, the existence of a specific legal framework for public administrations cannot be considered an obstacle when trying to achieve an adequate technical design for eGovernment services. This objective should be always pursued, even when there are no specific provisions.

5. What are the barriers remaining in this field?

5.1 Constraints imposed by the requirements of administrative procedures

Adopting administrative decisions through the appropriate procedure is such a key objective of Administrative Law that it means all unilateral decisions with legal implications must respect the appropriate procedure or regulation, except in some very isolated cases. There are two main justifications for this requirement: an appropriate satisfaction of public interests; and a guarantee of protection for citizens against administrative decisions that are taken in the exercise of very powerful, unilateral competences. As in the field of judicial procedure, the correct observance by public administrations of a legally predetermined sequence of steps must therefore be considered as a useful and necessary tool for adopting decisions in an objective and fair way.

In order to realize fully the potential benefits of using ICT to enhance efficiency in decision making and in establishing communications with citizens and companies, the implementation of electronic public services demands a higher level of streamlining and flexibility of rules and procedures than for traditional methods. For eGovernment services, these operations could be done automatically without a formal procedure or, instead, by following a more informal process than that fixed for those actions when carried out using traditional tools based on written documents and personal relationships. If the legal framework does not admit these particular typical features of eGovernment, then a serious problem for administrative decisions and communications is likely to appear because of a conflict between the speed that is allowed by ICT-enabled services and the formal requirements imposed by the traditional regulation of administrative procedures.

It is necessary to promote a review of this legal framework in the light of relevant technological change in order to avoid these negative consequences for the implementation on eGovernment services. Although this process is generally the responsibility of national authorities and, depending on the context, of regional and local governments, in certain cases the EU may influence the outcome positively when it has the competence to act in a particular field. For instance, the potential benefit of such a European influence has been clearly shown by Directives 2004/17/EC and 2004/18 on public procurement. This EU-wide regulation has been rapidly taken into account by many Member States, such as in France's adaptation of its own legal framework that goes even further than recommended by the Directives⁷. With a more general scope, the need for simplifying administrative procedures has also been recommended as a trend in public

⁷ As explained in the country examples of eProcurement section of our project's website (<http://www.egovbarriers.org/?view=example&example=procurement>).

needs for eGovernment services by a report from the European Commission's Institute for Prospective Technological Studies (Centeno, van Bavel and Burgelman (2004).

Some other relevant general initiatives in this area include: the European consultation on 'cutting red tape' and projects to reduce 'administrative burdens' launched by several Member States, including Sweden⁸, the Netherlands⁹, Spain¹⁰ and Denmark¹¹. A very interesting and useful approach to these problems has been adopted by the *Virk project* of the Danish Internet Portal for the Danish Commerce Sector, where the reduction of the administrative burdens has been achieved through a proactive methodology: when companies need to complete reports, the basic information is pre-filled because the portal shares data with the public registers¹².

Such simplifications of administrative procedures are one of the main priorities of citizens in these States with a continental model of public administration, as recently shown in France¹³. This indicates that the technological modernization of public administrations should be used to simplify the design of administrative procedures, which involves a historic transformation process that is much more than a question of changing from paper-based to digital media formats. The success of eGovernment from a legal point of view requires taking account of the importance of avoiding the establishment of stronger constraints on administrative activity when using ICT tools, unless such a course is reasonable in a particular context.

Administrative rules based on traditional and well-established legal principles are usually neither designed to promote the use of ICT nor prepared to allow it, since the appropriate technological innovations were merely imagined when the laws were passed or rules made. There may even be some provisions that are contrary to the use of ICT, such as a requirement for the use of certain types of paper document¹⁴, which create a clear and significant barrier. Nevertheless, such inconveniences can be overcome, for instance through a positive approach to technological change that interprets a legal silence on technology as an implicit authorization. Therefore, it is always necessary to assess whether a legal modification needs to be promoted to solve such problems, or whether only a different perspective is enough to overcome a perceived potential blockage to eGovernment (Johnssén 2003). To avoid this kind of uncertainty, Italy has recently passed broad legislation on eGovernment, the 'Codice dell'amministrazione digitale'¹⁵ that aims to contribute to removing 'obsolete norms' as obstacles to further eGovernment development. With a similar aim, the Slovenian Parliament modified the General Administrative Procedure Act in order to make available to citizens both the electronic sending of application and receipt of online administrative communications¹⁶.

These exemplify the importance of designing eGovernment services from the outset with the perspective of citizens as a prime consideration. If this is not done, legal obstacles could impede the adequate satisfaction of user needs, resulting in the requirement to solve resultant inconvenience at a later stage through legal changes. Consequently, when a modification of the legal framework is essential in order to adapt obsolete rules, it will be

⁸ <http://europa.eu.int/idabc/en/document/4362/330>

⁹ <http://www.administratievelasten.nl>

¹⁰ <http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=1818>

¹¹ <http://www.amvab.dk/>

¹² Further information on this project can be found at:

<http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=1867>

¹³ According to a survey by BVA (<http://www.bva.fr>), 60% of those polled declared this should be the main priority for public administration. Further information about this question can also be found at:

<http://europa.eu.int/idabc/en/document/4501/194>

¹⁴ This is the case with the Spanish Act on Legislative Promoting, which has recently been modified – (by Constitutional Law 4/2006) to allow the use of eSignatures.

¹⁵ Further information on this example can be found at:

<http://europa.eu.int/idabc/en/document/4820/5707>

¹⁶ Further information on the Slovenian project *e-serving* is available at:

<http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=315>

necessary to check which kind of decision is required and the relevant competent authority to promote it. If the regulation has been approved through a general Act, then a Parliamentary intervention will be indispensable, thereby involving a higher complexity in which the public administration concerned will not be able to overcome the barrier on its own. On the other hand, a rule whose modification has only an administrative range will be easier to change, especially if the competent authority belongs to the same public administration that is encountering the obstacle.

Related barriers: leadership failures, poor coordination, lack of trust.

5.2 Inadequate adaptation of administrative decisions regulation to ICT

Following on from the previous section, it is also important to note the latent tension between the possibilities offered by ICT capabilities and the formal requirements of Administrative Law. This poses a potentially significant barrier to which the general points made in Section 5.1.5.1 also apply. A clear demonstration of this confrontation can be seen in the legal conditions for the validity of administrative decisions, most of which require compliance through a paper-based document and with the direct intervention of a person and not a machine.

This indicates why the validity of administrative acts can be questioned when using ICT, since the observance of some essential formal demands may be impossible or, in some cases, contrary to the flexibility and speed offered by technology (Giroto 2002). In this context, a relevant risk for eGovernment can be seen to arise in some circumstances when it is not possible to place administrative decisions using digital media on the same level of validity and efficacy as those adopted by traditional means. The scope of this inconvenience, and the complexity of dealing with it, are illustrated by some related questions, such as: Can administrative decisions be 'adopted' by a computer and, if so, which kinds of decisions? Although it is obvious that discretionary powers must be put into practice directly by the competent authority, what are the limits for other public bodies dealing with an issue? Is it necessary that death certificates are directly drawn up by a civil servant?

One of the main conditions for the validity of administrative decisions is that they are adopted by the competent authority, which can be identified with a natural person who assumes the consequences of his/her action. This principle in the field of Administrative Law may be considered a relevant barrier for the implementation of eGovernment services because many decisions could be taken directly by ICT-enabled systems without a direct human intervention. In addition, from the point of view of the responsibility for the decision adopted, the use of ICT involves an essential problem of determining who must be considered the author of the administrative act and, therefore, responsible from a legal perspective (Marcou 2002). This raises inevitable questions about the legal conditions required to automate administrative activity, the strict limits that have to be respected if administrative decisions are to be considered valid and, if necessary, how to promote those legal modifications demanded by electronic public services.

Overcoming this obstacle requires a specific framework taking account of the singularities of eGovernment that could not have been considered when the rule was formulated. As that technology was not yet available, administrative activity was based on the use of paper and through personal relationships. The Spanish basic *Act on Administrative Procedure*¹⁷ offers a relevant example of the legal conditions imposed on the use of ICT in order to enable all public authorities at national, regional and local levels to exercise their competences. It includes a demand for prior approval of the software used for this purpose by the competent authority, who must publicize its technical characteristics. Thus, a direct link can be established between that authority and the administrative decisions adopted

¹⁷ This Act and other regulation related can be found at:
http://www.map.es/documentacion/legislacion/procedimiento_administrativo.html

through electronic means. Nevertheless, in this case an alternative solution may be pursued if there is no clear regulation related to this problem. Instead of adapting the current framework, public administrations can avoid the obstacle to validating administrative decisions by interpreting the general rules according to the requirements established by this Spanish Act. This is a hazardous solution from the legal security point of view and, in the last analysis, could be subjected to a judicial review to assess the fairness of the approach followed.

Related barriers: leadership failures, poor coordination, lack of trust.

5.3 Failure to reduce the administrative burdens relating to the conditions of administrative documents

As already indicated, one of the most significant concerns of European and national authorities regarding Administrative Law and eGovernment is to simplify the requirements for easing the so-called administrative burdens, particularly those aspects involving the inevitable exchange of information that demands the kind of networked operations highlighted as one of the main challenges to eGovernment in the report for *the* Institute for Prospective Technological Studies on eGovernment in the EU in the Next Decade (Centeno, van Bavel, and Burgelman 2004).

This is not only a question of efficacy from an internal administration perspective. It is also a relevant barrier when implementing inter-administrative electronic public services, where there can be an even wider significance if potential problems are not addressed successfully. Such inconvenience could be increased in the field of pan-European electronic services¹⁸, where information is provided by diverse public administrations subjected to heterogeneous legal frameworks that impose different requirements for administrative documents. The external conditions within which such services are designed, developed and used can be as important as the content of those services, for example in terms of legal tradition and culture not only the validity of particular ePublic Services (Yahiel 2002).

This indicates why the electronic exchange of administrative documents must respect any formal legal requirements in order to establish their validity and efficacy. If this is not done, the advantages of using electronic media will be counteracted by the legal conditions. To overcome this potential obstacle, one option is to simplify the formal requirements, although this is not always feasible.

A better solution is to establish an alternative way of providing the specified level of guarantee for the information contained in the documents in a way that has been fully adapted to the capabilities of ICT tools¹⁹, as in the Spanish *Act on Administrative Procedure* and the French Ordinance 2005-1516, adopted on 8 December 2005, which allow substituting traditional formalized written certificates for simple online transmissions of the information they contain. As this does not require necessarily any legal change, it can be adopted by each public administration, provided adequate technical measures are used, such as digital signatures and secured channels that guarantee the authenticity and integrity of the information²⁰. In a similar way, the Danish TASTSELV initiative has replaced the traditional paper-based tax application forms by a first draft that can be approved either by phone or via Internet. As most of the information has already been provided by third parties (e.g. employers, banks mortgage institutions, trade unions, social benefits administration), citizens can fulfil their tax obligations in a simpler and more efficient and

¹⁸ This was one of the most relevant topics examined in the small group discussion held in Brussels at a *Breaking the Barriers to eGovernment* project workshop on 29 September 2005.

¹⁹ At a basic technological level, this demands the interoperability of the software used by all the public administration concerned (see Section 5.7 on Relationships between Public Administrations, Citizens and Other ICT Actors).

²⁰ Unless specific demands are imposed by regulations applicable to certain documents.

accurate way as they have to check only if all the data are correct and, if necessary, report only very few details to pay the correct personal tax²¹.

A different solution has been adopted for certain pan-European services, such as the EURODAC²² centralized database for asylum application, which is based of the flexibility offered by Article 1.2 of Directive 95/46/CE for international exchanges of personal data. However, this option is not always possible at the national level if local legal limitations make it difficult to meet the requirements for implementing effective eGovernment services.

In addition, a minor but general change in the legal framework may sometimes produce relevant consequences that help to remove unnecessary obstacles that have had only a traditional justification. This is the case of the Spanish Royal Decree 522/2006 that has repealed all those previous regulations that demanded to append a copy of the Identification Card when sending an application form to a public authority²³. If this modification had been adopted, a serious obstacle to eGovernment services would have remained in force since the copy of the ID card would still be compulsory, regardless the way – electronic or not – chosen to contact the public administration. It addresses one of the main problems faced by the Czech Government in order to accept e-invoices, since the legal framework had not contained any reference to e-invoicing²⁴.

Related barriers: leadership failures, poor coordination, workplace and organizational flexibility, lack of trust

5.4 Lack of adaptation of technological regulations to the singularities of Administrative Law

Several relevant EU Directives have sought to modernize national legal frameworks in order to adapt their regulation to the special needs of the information society, especially in the fields of digital signatures and eCommerce. In this process, a strong influence of Private Law can be seen as a consequence of two main circumstances: when new regulations have been adopted with the clear economic purpose of facilitating the common market in certain sectors; and when relevant Directives have an effect on equivalent regulations in North American, which has a legal system where Administrative Law does not have a significant role. As a result, these Directives either have not included specific provisions for public administrations or their provisions are not sufficiently adapted to their particular needs from a legal perspective. This has made it necessary to apply private rules to the general process of technology change in public administration systems (Gautier 2002). These conditions may become an obstacle to the development of certain eGovernment services, for instance when a Member State has to adapt its national regulations to the requirements of these Directives, although Private Law principles may not be adequate enough for the administrative legal framework.

An illustration of difficulties that can be encountered relates to the provision in the Directive on digital signatures for a free certification service providing. This means that citizens and companies could use the certificates supplied by a service provider established in their own country in order to contact a public administration belonging to another Member State. However, although this Directive allows for some exceptions to its general rules for the public sector, certification has not yet been put in action generally due to the singularities and diversity of each national administrative context and the very important problems related to a lack of interoperability. These obstacles should be overcome by a future

²¹ A complete explanation of this project can be found at:

<http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=1814>

²² EURODAC involves a centralized database in comparing the fingerprints of asylum applicants and a system that enables each Member State to transmit data to this central record. For further information about this, see: <http://europa.eu.int/scadplus/leg/en/lvb/l33081.htm>

²³ The details of this project can be found at: <http://www.csi.map.es/csi/eModel/supresion.htm>

²⁴ Further information can be found at: <http://ec.europa.eu/idabc/en/document/5892/5920>

modification of the Directive that fixes clearer conditions for exceptions in the administrative field. Meanwhile, they can be solved by national authorities on the basis of the priorities of European Law.

On the other hand, the Directive on eCommerce is not applicable to public administrations, since its conceptualization of 'service' does not include public services. From this perspective, the limitations of liability for intermediary service providers do not affect those services offered by public administrations. This situation could be worrying to those States whose administrative systems are based on the direct and objective liability of public administrations. To address such concerns, national regulations should adapt the internal framework to the demands of this Directive to ensure public administration is subject to the same regimen as private intermediary service providers.

Related barriers: leadership failures, poor coordination, lack of trust

5.5 Failure to preserve guarantees to citizens when moving to the use of electronic media to deliver public services

The tension between administrative efficiency and the protection of the rights of citizens and companies when adapting Administrative Law regulations to the specific requirements of using ICTs can result in an over-emphasis on the needs of the public authorities that dominate regulatory and legal decision making. A lack of adequate adaptation also carries a risk, since many of the traditional rules take account only of personal contacts but not online communications (Prins 2002).

Administrative Law may be ignored if it is not suited to the concrete and real circumstances in which it must be applied, for example if it would mean technological capabilities are given greater weighting than citizens' rights in implementing eGovernment services (Lessig 1999) and therefore be disadvantageous for citizens and companies when they engage in online relationships with public administrations. To ensure that the rights of citizens and businesses when using electronic media are guaranteed, at least to the same level as if traditional means were being used, regulations relating to interactions with public bodies must therefore be adapted appropriately to take specific account of the use of ICT-based tools. If there is an unfair lowering of the level of protection when using electronic media, many citizens and businesses could lose interest in eGovernment services, even for those from which they could benefit substantially.

For example, in the past when a citizen wanted to deliver an application form to a public administration, he/she would typically have gone to an administrative building and to the appropriate desk, where a civil servant would issue a receipt to prove the document has been handed over and, if necessary, give a warning if there are certain problems with the form. When that action is made through Internet, there is no direct personal response since nobody is waiting on the other side of the Net. On the other hand, when a public administration wants to notify its decisions to relevant parties, the specific rules regarding this kind of administrative communication must be observed since the effectiveness of those decisions may be affected, for instance when the specification of a time-scale to lodge a judicial appeal does not start until the notification has been correctly made.

Consequently, public administrations should be legally obliged to give all the necessary information online in order to deal adequately with application forms delivered through electronic means, particularly when that possibility has been recognized as a right. Administrative websites must warn citizens and businesses of any mistakes during this process and an immediate digital receipt must be drawn up and delivered to the relevant party. For notifications of administrative decisions, the absence of a personal contact demands a particular legal regulation to guarantee the correct reception of this kind of communication, especially to indicate the consequences of a technical mistake when trying to undertake the necessary actions notified. Public administrations can adopt these measures even if there are no legal obligations to do so, but in such cases citizens will not

have their rights protected at the same level as when using an alternative to eGovernment services.

Related barriers: leadership failures, digital divides and choices, poor coordination, lack of trust

Sources

Publications

- Centeno, C., van Bavel, R. and Burgelman, J-C. (2004), eGovernment in the EU in the Next Decade: The Vision and Key Challenges, Technical Report EUR 21376, Brussels: Institute for Prospective Technological Studies, European Commission, <http://europa.eu.int/idabc/servlets/Doc?id=19131>
- Chatillon, G (2002), 'Responsabilité et Administration Électronique: Une Notion Revisitée', in Chatillon, G. and Marais, B. du (2003), Administration Electronique au Service du Citoyens, Brussels: Bruylant.
- Danish Commerce and Companies Agency (2005), Better E-governance. A Measure of E-governance in New Danish Laws, <http://ec.europa.eu/idabc/en/document/4295/333>
- Fromont, M. (2006), Droit administrative des États européennes, Paris: PUF
- Gautier, P. Y. (2003), 'L'adaptation de Solutions de Droit Privé à l'administration Numérique', in Chatillon, G. and du Marais, B., Administration Electronique au Service du Citoyens, Brussels: Bruylant, 2003
- Girot, C. (2002), 'France', in Prins, J. E. J. (ed), e-Government and its Implications for Administrative Law: Regulatory Initiatives in France, Germany, Norway and the United States, The Hague: Asser Press
- Gross, T. (2001), The Legal Framework for eGovernment, Centre for Media and Interactivity, University of Giessen, available at: http://mediakomm.difu.de/documents/kongress/esslingen/gross_en.pdf
- Johnssén, G.(2003), To Regulate Or Not To Regulate. E-government, Administrative Law and Change, available at: <http://www.skriver.nu/esociety/archives/gj2.PDF>
- Lassnig, M., Markus, M., and Strasser, A. (2004), eGovernment – the Regional Dimension, Biser Domain Report No. 1, available at: http://www.biser-eu.com/10%20Domains%20Report/BISER_eGovernment_fnl_r.pdf
- Lessig, L. (1999), Code and other Laws of Cyberspace: How Will the Architecture of Cyberspace Change the Constitution, New York: Basic Books
- Marcou, G.(2002), 'Le régime de l'acte Administratif Face à l'électronique', in Chatillon, G. and du Marais, B., Administration Electronique au Service du Citoyens, Brussels: Bruylant, 2003
- Prins, J. E. J. (2002), Taking Administrative Law into the Digital Era: Regulatory Initiatives in France, Germany, Norway and the United States, The Hague: TMC Asser Press and Norwell, MA: Kluwer Law International.
- Valero, J. (2004), Régimen Jurídico de la e-Administración, Granada: Comares
- Yahiel, M. (2002), 'Des Formulaires en Lingne aux Téléprocédures', in Chatillon, G. and du Marais, B., Administration Electronique au Service du Citoyens, Brussels: Bruylant, pp. 31-37.

International and European-level Legislation, Regulations, Conventions and Treaties

Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities L 13, 19/01/2000, pp. 12-20, <http://europa.eu.int/ISPO/docs/policy/docs/399L0093/en.pdf>

Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities L 178, 17/07/2000, pp. 0001-0015, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML>

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Communities L 201, 31/07/2002, pp. 37-47 ('Directive on privacy and electronic communications'), http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

Directive 2004/17/EC of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, Official Journal of the European Union, L 134, 30/4/2001, pp. 1-113, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

Directive 2004/18/EC of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, Official Journal of the European Union, L 134, 30/4/2001, pp. 114-240, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en01140240.pdf

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, 23/11/1995, pp. 0031-0050, http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

Websites

eGovernment Good Practice Exchange (<http://www.epractice.eu/>).

IDABC, the service for the Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens to help enable the use of information and communication technologies to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe (<http://europa.eu.int/idabc>).

Paper 2: Authentication and Identification in eGovernment

Dr Sjaak Nouwt

Tilburg Institute for Law, Technology and Society (TILT), University of Tilburg, Netherlands

1. Description of this legal area

The topics that described here are 'authentication' and 'identification'. Authentication in an eGovernment context is typically an act of establishing or confirming someone or something as authentic, involving any process through which one proves and verifies certain information. Identification is an act of establishing or confirming the identity of a person. The difference can be illustrated by the example of someone logging on to a shared account on a computer. This person will not be uniquely identified, but can be authenticated as one of the users of the account through the use of a shared password. On the other hand, identification does not necessarily authenticate the user for a particular purpose.²⁵

Authentication is used for the procedure of guaranteeing the origin and the integrity of electronic information (Dumortier 2002). A 'digital signature' can be used to secure electronic information in a way that enables verification of both the originator and the integrity of the information. This is a type of electronic signature that uses 'public key cryptography', in which the author of electronic information can 'sign' this information with a secret cryptographic key (which must always be kept private by the user). The signature can be verified only with the associated key of the author that has been made public, so is known as the 'public key'. This authentication procedure can therefore confirm a user's identity by verifying the possession of the secret key the author has used to encrypt the information. The recipient checks the identity of the author by decrypting the information with the public key of the author.

Authentication and identification can be considered elements of the broader concept of 'identity management', which arises because of the need for governments to authenticate online users (NECCC 2002, p. 35). As authentication is needed to avoid or reduce the risk that the wrong person will access, use, change, delete or otherwise improperly interact with valuable data or transactions, authentication and identity management can be considered elements of legal risk assessments and risk control measures.

2. How is the area of Authentication and Identification related to barriers to eGovernment?

Many non-electronic transactions between government and citizens or businesses are concluded with a signature, such as to authorize receipt of a welfare payment or sign a cheque. When services are moved to the electronic world, the need emerges for an equivalent electronic means to ensure:

- the authenticity of each party within the electronic communication;
- the integrity of the contents of the communication; and
- the electronic communication can be confirmed if there is a dispute.

The process of authentication relies on the accessibility of the public keys of the users to all the communication partners. It also relies on the trusted relationship between the

²⁵ RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1, Chapters 2.2.2 and 2.2.5 (see: <http://www.rsasecurity.com/rsalabs/node.asp?id=2152>).

identity of the users and their public key. Furthermore, the authentication procedure is based on the presumption that the public key really belongs to the signer. There is a risk that somebody creates a key-pair, places the public key in a public directory under somebody else's name and signs electronic messages in the name of somebody else.

Another risk is that the public key does not belong to the claimed identity, as a public and private key pair has no inherent association with any identity because it is simply a pair of numbers. To limit these risks, there are third parties (called 'certification authorities') that certify public keys by guaranteeing the relationship between the identity and the public key through the use of a "digital certificate". It is important that this third party is accepted by all users as impartial and trustworthy.

A significant barrier to the use of electronic communications and electronic commerce and government may be created by divergent national rules with respect to the legal recognition of eSignatures and the accreditation of providers of certification services as being able to offer these signatures. In this respect, the primary aim of Directive 1999/93/EC of 13 December 1999 (the 'eSignatures Directive') is to create a "harmonized and appropriate legal framework for the use of electronic signatures within the Community and to establish a set of criteria which form the basis for legal recognition of electronic signatures". However, it is necessary to further clarify two main areas. One is the open norms laid down in the eSignatures directive. The other is to examine how theory and practice can be better tuned and whether the law can create solutions to overcome obstacles relating to the balance between costs and benefits in the use of digital signatures.

According to a report on the legal and market aspects of eSignatures (Dumortier et al 2003), Directive 1999/93/EC sets very high requirements on secure signature-creation devices. Such devices still rarely find their way to the market. The authors plead for more flexibility for these legal requirements in the future, arguing that otherwise the high legal requirements could be a barrier to eGovernment.

However, there is a general question about whether such legal requirements are real barriers for eGovernment initiatives. Failure to meet a legal requirement does not necessarily prevent someone from taking the first step to eGovernment initiatives. These can be taken and eGovernment services resulting from them can be delivered even when the initiative is not fully in compliance with the law. The initiator can deliberately take the risk that the initiative will be taken to court, with the service being delivered provided the case is not ruled illegal in court.

Divergent national rules with respect to the legal recognition of eSignatures and the accreditation of certification-service providers may create a significant barrier to the use of electronic communications and electronic commerce and government.

3. What is the European context for this area, including legislation, policy statements, institutional arrangements relevant to this topic?

On 13 December 1999, Directive 1999/93/EC on electronic signatures was signed, and published in the Official Journal of 19 January 2000. From that date, the EU member states had 18 months time to transpose the Directive into their national law (Dumortier 2002).

This eSignatures Directive is an example of co-regulation at European level. The Directive itself defines only the general principles, which must be further specified by self-regulatory mechanisms, mainly by technical standardization. At the end of 1998, the European Commission issued a mandate to the European standardization bodies (CEN/ISSS²⁶, CENELEC²⁷ and ETSI²⁸) to analyse the future needs for standardization activities in

²⁶ See: <http://www.cenorm.org/cenorm/index.htm>

²⁷ See: <http://www.cenelec.org/>

²⁸ See: <http://www.etsi.org/>

support of essential legal requirements related to eSignature products as stated in the (then draft) directive. To meet the requirements of the Commission mandate, the ICT Standards Board (ICTSB)²⁹ launched the European Electronic Signature Standardization Initiative (EESSI), which published in July 1999 an expert report (Nilsson et al 1999) about future standardization requirements at a European level. Based on this report, EESSI approved a work programme with a division of tasks between CEN and ETSI. In the months that followed, intensive work has been performed in the area of standardization of electronic signatures, with a first set of deliverables given to the European Commission on 3 April 2001.

References to the required standards were published in the Official Journal in July 2003. These are part of a longer set of specifications defined by EESSI and are included in their work programme. With the publication of this full set of standards, EESSI has fulfilled its mandate and consequently ICTSB decided to close EESSI WG in October 2004.³⁰ However, standardization work in this area is still ongoing by CEN members, and by ETSI TC/ESI, but at a lower level of activity. Remaining coordination tasks in the area of electronic signatures are now carried out by the Network and Information Security Steering Group (NISSG) of ICTSB.

The existence of a European legal framework regarding digital signatures is no guarantee that this field of law no longer entails any barriers to eGovernment. In this respect, reference can be made to an earlier study on the legal and market aspects of electronic signatures conducted for the European Commission (see Dumortier et al 2003). The report on this research shows that much work still needs to be done in the field of eSignatures before their pan-European use can be expected. For example, divergent rules still exist within the EU because of different interpretations regarding the eSignatures Directive. The report concludes that the text of the Directive is adequate enough to serve its purpose in the near future, but that it needs re-interpretation and clarification. A subsequent conclusion of relevance to our project is that without this re-interpretation and clarification, barriers to eGovernment related to eSignatures will remain. Clarification is needed, for example, with regard to supervision schemes, voluntary accreditation and the public sector exception.³¹ National rules regarding the recognition of foreign qualified certificates may also still pose a barrier to eGovernment across state boundaries.

In some instances, the report even explicitly refers to eGovernment (Dumortier et al 2003: p.12): "It is necessary to perform a more detailed study on the Internal Market consequences for eGovernment programmes of the Member States. There is a clear danger that these programmes will result in national barriers, fragmentation and interoperability. Efforts towards improvement of interoperability between eGovernment programmes and particularly between their electronic signature applications should be supported or initialized at a European level."

National barriers, fragmentation, and interoperability are also dangers that can be caused by the variety of eSignatures issued in different Member States. Some EU Member States are using electronic identity cards for several purposes (e.g. Belgium, where people can pay taxes through the internet). Sometimes, these electronic id-cards are only issued to the citizens of the related country (in the case of Belgium) or to the residents (inhabitants) of the specific country (in the case of electronic id-cards in Germany). As a result, a German who lives in Belgium is ineligible to use the electronic id-card system in both Belgium and Germany, and therefore unable to benefit from the electronic id-cards in both countries. This danger for national barriers, fragmentation, and interoperability is also caused by the fact that the issuance of electronic id-cards is a Third Pillar activity, which falls solely under the national sovereignty of the Member States. Therefore, the exclusive jurisdiction can be considered a barrier for the use of electronic id-cards across national borders. Harmonization of eSignatures is hence not only necessary as to the format which

²⁹ For more on ICTSB, see <http://www.ictsb.org>

³⁰ See: http://www.ictsb.org/EESSI_home.htm

³¹ Directive 1999/93 has a so-called 'public sector exception' in article 3.7 which allows Member States to use electronic signatures in the public sector subject to possible additional requirements.

parties will have to use, but also with regard to the parties (in this case the various EU Member States) that issue the various eSignatures.

Another interesting point in the report was the conclusion that a clear need exists for regulation dealing with archival service providers, or with registered mail services. From a user's perspective, it is difficult to understand why such services remain completely unregulated, while a complex regulatory framework has been established for issuers of certificates. It is therefore recommended to undertake studies about the need for regulation with regard to other categories of trust services (see for example the European Commission's 2003) first report on the application of Directive 2000/31/EC (the 'electronic commerce Directive')³².

A central source of disagreement among scholars and lawmakers is about whether the laws governing electronic signatures should remain neutral towards technology or attempt to specifically regulate currently favoured technologies. In this respect reference can be made to the following statement of Barofsky (2000): "Digital signatures are not the only available form of secure electronic signature. 'Signature dynamics' combines biometrics and cryptography to create signatures that securely attach unique characteristics of an actor's character or behaviour to an electronic document. Signature dynamic methods of authentication have the advantage of being bound to the signatory rather than to the document. This feature eliminates the need to go through a trusted third party or a CA to link an electronic signature to an individual. Favouritism toward digital signatures risks excluding other possibly superior technologies from entering and competing in the marketplace."

The main problem is that in jurisdictions that have enacted laws specific to certain digital signature techniques, it is not clear whether an electronic message signed by any method other than a digital signature is valid. Under the current eSignature Directive, a business using an otherwise "secure" signature method that is not a digital signature subject to a qualified certificate risks creating an unenforceable or voidable contract. This problem is aggravated by the fact that business and government choose methods for signing their computer documents that meet their own commercial and administrative needs. In the Netherlands, the DigiD (Digital Identification) system started on 1 January 2005 employing a username and password systems to identify citizens when they access online eGovernment services. However, questions have been raised about whether it complies with the requirement for an advanced eSignature, for example with the Dutch Society of Information Security (GvIB) reporting in April 2006 that it is too weak a mechanism of authentication to make it appropriate for application to tax forms.

A final point to mention is that high standards required by the Directive with regard to digital signatures has led to a system in which the costs do not outweigh the benefits. This is true not only for customers, but also for certification service providers. Therefore, although the digital signature system may seem to be efficient in theory, in practice its complexity and cost could be a drawback and potential blockage to some eGovernment developments.

At a Kennedy School Workshop on Digital Identity (Camp 2003), seven critical problem areas for an identity management discussion were identified.

- information architecture and management strategy;
- privacy and personal information protection;
- government policies;
- accountability inside and outside the system;
- metrics for design and evaluation;
- implementation of the infrastructure; and

³² See: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2003/com2003_0702en01.pdf

- roll-out and enrolment phase.

Each problem area has many independent and related research topics. Together, these make up a research space in which each problem area offers many individual questions to be addressed, both qualitatively and quantitatively. Camp subdivides these topics into six academic disciplines: Computer Science and Engineering; Management Information Science; Organizational Science; Economics; Social Sciences; and Law. For the legal discipline this means that significant changes to current authentication practices will implicate current legislation on individual rights, administrative responsibilities and organizational liability burdens (Camp 2003: p. 25).

4. What is the relationship of Authentication and Identification to the seven barrier categories and associated research questions?

4.1 Leadership failures (significant)

At first sight, the issue of authentication and identification does not seem to be relevant for this category of barrier. However, a lack of leadership could result in slow development and implementation of authentication and identification processes. This is illustrated by examples from different countries. For instance, from 2003 a Certificate of Residence can be obtained electronically in Austria by using an electronic signature on a smart card. Despite advances in technology, an online authentication technology like DigiD, which is being used in the Netherlands, has been criticized as being unfit for some eGovernment purposes. Knowledge and vision on technological developments seems to be important elements for leaders to guarantee the use of state-of-the-art authentication and identification processes.

4.2 Financial inhibitors (significant)

The use of a secure electronic signature, or even the combination of electronic signatures with biometrics, could be rather expensive. It seems clear that higher security demands result in higher costs for authentication and identification. In this context, a relevant question for this project is: Do the costs of providing effective security and trust systems could outweigh the benefits by raising the overall entry point for affordable investments? The advantages of having secure and trustworthy systems offered by government, such as improved trust among users and greater efficiency, will be weighed against the costs of investment. The result will show how much trust in eGovernment is worth in Member States. At a pan-European scale, investments in effective, secure and trustworthy systems might be better affordable than at a national level.

4.3 Digital divides and choices (significant)

Authentication and identification processes should be easy to use and not too expensive to apply, so a process like a digital signature should not be too expensive for an organization to apply or too difficult to be used by any of its customers. Otherwise, a digital signature could result in digital divides.

4.4 Poor coordination (very significant)

As illustrated above, despite the existence of eSignature Directive 1999/93/EC, a lot of work needs to be done to establish a pan-European use of electronic signatures. Within EU Member States, different rules still exist because of different interpretations of the Directive's provisions. This has also resulted in the failure to agree and implement

standards for electronic signatures. Therefore, despite the harmonization efforts attempted through several Directives, the following questions need to be discussed:

- Are there provisions in Directives that hinder the effectiveness of administration activity at different levels or have become a barrier for the competitiveness of the European economy, and how can they be altered to remove any blockages?
- Has the European framework on electronic and digital signatures achieved greater trust in secure information exchanges by overcoming critical variations across the EU? If not, what further initiatives would be required?

In this respect, the European Commission (2006) concluded in its report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures that a “strategic role of eGovernment is recognized in the i2010 initiative, which fosters the deployment and efficient use of ICT by the private and public sectors”. According to this report, “the Commission will continue to encourage the development of e-signatures services and applications and will monitor the market. Beyond the support through eGovernment activities, particular emphasis will be on interoperability and cross-border use of electronic signatures. The Commission will encourage further standardization work in order to promote the interoperability and use of all kinds of technologies for qualified electronic signature in the internal market. It will prepare a report on standards for electronic signatures in 2006.

4.5 Workplace and organizational inflexibility (significant)

When authentication and identification processes are introduced in an organization, management and staff could resist such innovations. In some cases, their resistance could be legitimized by laws. For example, when the introduction of authentication and identification processes result in the processing of personal data from employees, the consent of the relevant Works Council could be needed. More generally, the question is raised about ways in which the current structure of Employment Law in Member States act as a blockage or facilitator for any restructuring of the public sector labour market that may be needed to realize the full benefits from high levels of ePublic Services delivery and use?

4.6 Lack of trust (very significant)

As in eCommerce, trust is an important enabler for eGovernment, especially because governments often process highly sensitive personal data from their citizens. Therefore, it is also of great importance that access to those personal data is highly secured, with the support of advanced authentication and identification procedures. In this context, the following research questions will be addressed:

- What delays in eGovernment developments have been caused by an absence of standards in approaches to identification of an individual or other unit, and the verification or authentication of that identity, that are essential to public service transactions – such as receiving welfare benefits, voting or paying vehicle-related charges? What blockages need to be removed in order to establish standards of identification and verification for pan-European online services?
- What obstacles have there been to wider use of electronic and digital signatures, in addition to any harmonization issues across Europe?
- How does fear of identity theft, fraud or error affect citizens' willingness to use eGovernment services?

4.7 Poor technical design (very significant)

The report by Dumortier et al (2003: p. 12) on legal and market aspects of eSignatures recommends the standardization of the European 'Qualified Electronic Signature'³³, which should give users a presumption that an electronic signature which complies with this standard will be presumed equivalent to handwritten signatures throughout Europe. Such a Qualified Electronic Signature would be especially useful for cross-border transactions in Europe. Therefore, in this context, a key question to be addressed is: Does a lack of standardization or interoperability of electronic identification and authentication technologies remain a barrier to eCommerce applications in the public sector?

5. What are the barriers remaining in this field?

5.1 The unavailability of a secure authentication process

The availability of a secure authentication process (such as DigiD in the Netherlands) is an important success factor for eGovernment (Cap Gemini and TNO 2004: p. 32). However, the use of different identity management systems in the Member States will certainly lead to interoperability problems at a European level. As a result, this is a real barrier to be considered, for example in relation to laws or the legislation process regarding secure authentication and privacy.

Some organizations have set up their own procedures instead of waiting for national standards for secure authentication. It therefore seems that legislation is needed to create a pan-European standard identity management system for authentication and identification. It has also been recommended in the Dumortier Report, that a more detailed study is necessary on the Internal Market consequences of the eGovernment programs of the Member States. The report warns that the "clear danger that these programmes will result in national barriers, fragmentation and interoperability" means support must be given to the interoperability between electronic signature applications at a European level. The reliability of digital identifiers for identity management is of great importance for eGovernment services, and a government must be able to authenticate its citizen's claims about their identities to fulfil its fundamental tasks.

According to the European Commission (2006) report on the operation of the eSignature Directive, problems exist with regard to mutual recognition of eSignatures and interoperability. Thus, the Commission is organizing a series of meetings with the Member States and the relevant stakeholders to address a number of issues with the view of considering complementary measures where appropriate, including:

- differences in the transposition of the Directive;
- clarifications of specific articles of the Directive; and
- technical and standardization aspects; interoperability problems.

At a European level, eGovernment needs a secure and uniform identity management system, which could be met by drafting appropriate legislation at a European level to create a relevant pan-European standard.

Related barriers: leadership failures and poor coordination at a pan-European level and poor technical design at a national level.

³³ This is an advanced form of electronic signature (as defined in the eSignature Directive) based on a qualified certificate. This is created by a devices that can create a secure signature as described in Article 5.1 of this Directive (see: http://portal.etsi.org/esi/esi_faq.asp).

5.2 Governments uncertainty about identity management systems

Uncertainty about identity management systems might be a perceived barrier. Governments and government agencies are not always certain about the legal acceptability of an identity system (like an eSignature) because of poor coordination in this field. Furthermore, the lack of interoperability of such identity systems could be a barrier, which can result from poor technical design. Although legislation exists at the European level (Directive 1999/93/EC), its implementation throughout Europe should still be streamlined (Dumortier et al 2003: p.13).

To overcome blockages created by this barrier, Directive 1999/93/EC should be re-interpreted and clarified (Dumortier et al 2003: p 9). However, at the same time national governments and government agencies require more clarity about which kind of identity systems can be used, for example whether a Qualified Electronic Signature should always be used or whether better alternative technologies are available. These requirements demand effective leadership at an international level.

The lack of interoperability has also been identified as a big obstacle for acceptance and the proliferation of electronic signatures (Dumortier et al 2003: p. 8), particularly for eGovernment services at a pan-European level. As a result, many isolated systems of electronic signatures exist. Therefore, it is important to promote interoperability of identity management systems (electronic signatures). It seems questionable whether this should be promoted by harmonizing legislative measures. However, one way or another, it seems important that the European Commission encourages the work on standardization of the technologies behind identity management systems, while at the same time leaving space for alternative technologies to a standardized system, such as Qualified Electronic Signatures (Dumortier et al 2003: p.13).

The legal acceptability of different identity management systems should be clarified. It does not seem necessary to do this by drafting new legislation. The interoperability of national identity management systems should also be promoted at a European level. This seems possible by encouraging the standardization of technologies. It is not clear yet whether legal change or additional legal measures are necessary in this respect, or if the existing legal framework is sufficient.

Related barriers: leadership failures, poor coordination, poor technical design.

5.3 Identity theft

Identity theft refers to crimes and misdeeds perpetrated using the personal information of another (Camp 2003: p. 10). It involves the risk of losing one's digital identity through error, misuse or an identity abuse (such as identity theft or identity fraud) or because of the unauthorized access, modification, deletion or transmission of sensitive, high value or mission critical data and systems in commerce. It is a particularly significant real barrier to eGovernment for the end-user consumer or citizen (NECCC 2002: p. 38).

Identity theft is caused by weaknesses in identity management systems (often as a result of poor technical design), combined with the increasing availability of personal information. There is consensus that identity theft is a large and growing problem. For instance, Camp (2003: p.10) estimated that annually between one quarter and three quarters of a million people in the US are victims of identity theft. A private research company also estimates that seven million Americans were victims of identity theft in 2002.

In the Netherlands, a Bill to introduce a general citizen service number, the Burger Service Nummer (BSN), was adopted on 12 September 2006 by the Dutch House of Representatives and will be used by every Dutch government agency from 1 January 2007. This would make it possible to combat fraud. At the same time, it increases the

citizens' vulnerability as the more value that is added to a general identifier the more will swindlers be interested in it. When government agencies have a blind faith in such a citizen's service number, they could also have too much trust in the false identity of a swindler.

It is quite a challenge for a citizen to prove his identity when his or her major identifying documents have been compromised. Information can linger in computers until manually removed, and many decisions are made by silently and automatically consulting databases. An individual may never know whether they have completely secured their identity. Technical and legal protection against identity theft is therefore important for gaining and keeping the trust of citizens in eGovernment.

For misusing others' personal information, penalties have to be threatened and enforced for accountability mechanisms to work. Misuse can be malicious, by a government official or by a private party, but personal information can also be misused by mistake. Furthermore, individuals can act irresponsibly with their own data. One question is whether the legal system should pursue all kinds of disruptions of the security of an identity management system, including cases when an individual accidentally compromises the security of the system. To avoid such a legal issue, the identity management system should be made secure against the loss or abuse of data within it.

The question of whether legal changes are necessary should be further researched. At least for pan-European eGovernment initiatives, harmonization of national legislation is necessary.

Related barriers: poor coordination, poor technical design, lack of trust, leadership failures, financial inhibitors.

5.4 Citizens' uncertainty about identity management systems

Another perceived barrier on the demand side might be the uncertainty of citizens regarding the integrity and authenticity of an eSignature-based identity management system. Uncertainty about the reliability of this system and about data sharing between governments can result in a lack of trust in online government.

Trust is critical for any such relationship between government and citizens (e.g. see Camp 2003). The development of sufficient trust in eGovernment requires a reliable identity framework. An individual must be confident in the relevant attributes of other parties in the relationship. According to the Dutch Professor Bart Jacobs³⁴, the electronic environment should authenticate itself to the citizen first, before the citizen is able to access a public service. Confidence is also based on establishing good and reliable reputations.

The importance of electronic identification and authentication was stressed by the respondents in the Your Voice on eGovernment 2010 survey (European Information Directorate General 2006). According to 65% of the 232 respondents, the most important issue European eGovernment should focus on is "electronic identification and authentication". In addition, rather than preferring a single European scheme, most of the respondents think, that the use of the national electronic identification schemes should be enabled in transactions with other Member States. Consequently, most of the respondents think that the mutual recognition of electronic identities should be provided by Member States.

Lacking interoperability was considered as the main barrier in the area of electronic identification and authentication (58% of 150 respondents). The second most important

³⁴ Professor of Software Security and Correctness, Radboud University Nijmegen, and Professor of Design and Verification of Secure Software Systems, Technical University Eindhoven, the Netherlands (see: <http://www.cs.ru.nl/~bart/>).

barrier was still national legislation (51%). Other highly rated barriers were lack of awareness of benefits (43%) and lack of trust and security, whether perceived or real (also 43%).

Identity management may also involve pseudonymous or anonymous systems. Either approach to managing personal identifiers can improve trust in eGovernment, provided the chosen approach is implemented properly. The Workshop on Digital Identity (Camp 2003) called for policy shifts relating to identity management after exploring various future scenarios relating to identity theft and loss of privacy. Such shifts include gaining greater awareness of the scope of identity theft problems and real or assumed loss of privacy, including a better understanding of what identity management must do and also what it cannot do.

In this respect, individuals should be able to manage various existing identities of themselves involving various tokens and authorizations (NECCC 2001: p. 31), such as nickname in some particular social contexts (e.g. a professional designation for work purposes and a stage name for a hobby rock band).. It is also understandable that people want to separate their different identities by using different email addresses for work and for private purposes, business cards for different employers and other identity credentials for each name and corresponding realm of identity. At the same time, this may lead some people to create a personal file containing all the various usernames, passwords, system preferences, and other relevant information needed to keep grip on the identity systems in which a person participates. A number of years ago, it was proposed in the Netherlands that the citizen would use a 'digital safe' for these purposes. However, a number of government agencies would also have access to this kind of personal and confidential information. In 2005, the Dutch government decided to realize a Personal Internet Page (PIP)³⁵ for every Dutch citizen.

At a European level, eGovernment needs to establish trust among citizens and other users in the integrity and authenticity of the identity management system that is employed. This should consider offering the possibility of pseudonymous or anonymous systems. However, because of digital divides, the use of such systems might vary to give citizens choices appropriate to their particular needs. Some form of legal protection against identity theft and protection of privacy should be sufficient to help address related problems.

Related barriers: leadership failures, digital divides and choices, poor coordination, lack of trust, poor technical design.

Sources

Publications

Barofsky, A. (2000), 'The European Commission's Directive On Electronic Signatures: Technological "Favoritism" Towards Digital Signatures', *Boston College International & Comparative Law Review*, 24(1), pp. 145-60,
http://www.bc.edu/bc_org/avp/law/lwsch/journals/bciclr/24_1/24_1_TOC.htm

Camp, L. J. (2003), *Identity in Digital Government: A Research Report of the Digital Government Civic Scenario Workshop*. Convened by L. J. Camp and sponsored by National Science Foundation and the Kennedy School of Government, Kennedy School of Government, Cambridge, MA: Kennedy School of Government, Harvard University,
http://www.ksg.harvard.edu/digitalcenter/conference/identityReport12_31.pdf

Cap Gemini and TNO (2004), *Does e-Government Pay Off?*, November,
<http://europa.eu.int/idabc/en/document/3818/5666>

³⁵ Persoonlijke Internet Pagina – Advies Overheid.nl (update August 8, 2006). See: <http://advies.overheid.nl/4153/> and <http://www.e-overheid.nl/sites/pip/>

- Dumortier, J. (2002), 'Directive 1999/93/EC on a Community Framework for Electronic Signatures', in A. R. Lodder and Kaspersen, H. W. K. (eds.), eDirectives: Guide to European Union Law on E-Commerce, The Hague/London/New York: Kluwer Law International.
- Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., Van Eecke, P. (2003), The Legal and Market Aspects of Electronic Signatures. Legal and Market Aspects of the Application of Directive 1999/93/EC and Practical Applications of Electronic Signatures in the Member States, the EEA, the Candidate and the Accession Countries, Leuven: ICRI, http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf
- European Commission (2003), First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, COM (2003) 702 final, Brussels: European Commission, 21 November, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2003/com2003_0702en01.pdf
- European Commission (2006), Report on the Operation of Directive 1999/93/EC on a Community Framework for Electronic Signatures, COM (2006) 120 final, Brussels: European Commission, 15 March, http://europa.eu.int/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf
- European Information Directorate General (2006), Your Voice on eGovernment 2010, Online Public Consultation October – December 2005, V1.0, January, Brussels: European Information Directorate General.
- NECCC (2002), National Electronic Commerce Coordinating Council, Identity Management. A White Paper Presented at the NECCC Annual Conference, December 4-6, 2002, New York, NY. http://www.ec3.org/Downloads/2002/id_management.pdf
- Nilsson, H., Van Eecke, P., Medina, M., Pinkas, D. and Pope, N. (1999), European Electronic Signature Standardization Initiative (EESSI). Final Report of the EESSI Expert Team, 20 July, <http://www.ictsb.org/EESSI/Documents/Final-Report.pdf>

International and European-level Legislation, Regulations, Conventions and Treaties

- Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities L 13, 19/1/2000, pp. 12-20, http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf
- Directive 2000/31/EC of 8 June 2000 on certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities, 17/7/2000, L 178, pp. 1-16, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2003/com2003_0702en01.pdf.

Websites

- CEN, the European Committee for Standardization (<http://www.cenorm.org/cenorm/index.htm>)
- Cenelec, the European Committee for Electrotechnical Standardization (<http://www.cenelec.org>)
- eContent Programme for European Digital Content on the Global Networks, supporting the development of multilingual content for innovative online services across the EU (<http://cordis.europa.eu/econtent/>).

Europe's Information Society Thematic Portal on EU Culture and Society, eGovernment section (http://europa.eu.int/information_society/soccul/egov/index_en.htm)

eTEN, European Community Programme to help the deployment of eServices with a trans-European dimension, focusing strongly on public services in areas where Europe has a competitive advantage
(http://europa.eu.int/information_society/activities/eten/index_en.htm)

ETSI, the European Telecommunications Standards Institute (<http://www.etsi.org/>)

ICTSB, ICT Standards Board (<http://www.icts.org>)

IDABC, eGovernment Observatory (<http://ec.europa.eu/idabc/en/chapter/140>)

Information Society Technologies (IST), European Commission research programmes (<http://cordis.europa.eu/ist/>).

RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1, Chapters 2.2.2 and 2.2.5 (<http://www.rsasecurity.com/rsalabs/node.asp?id=2152>).

Research projects

European Commission Study, The Legal and Market Aspects of Electronic Signatures – Legal and Market Aspects of the Application of Directive 1999/93/EC and Practical Applications of Electronic Signatures in the Member States, the EEA, the Candidate and the Accession Countries',
http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

eGovernment Observatory, eGovernment in the Member States of the European Union, <http://ec.europa.eu/idabc/servlets/Doc?id=21035>

Paper 5: Intellectual Property Rights (IPR) and eGovernment

Dr Collette Cuijpers and Dr Sjaak Nouwt

Tilburg Institute for Law, Technology and Society (TILT), University of Tilburg, Netherlands

1. Description of this legal area

Many electronic services provided by governments relate to the dissemination of information. Governments can electronically disseminate information to their citizens as well as requiring citizens to provide information through an electronic medium. The Intellectual Property Rights (IPR) that apply to this information exchange are given to people to protect their creative works. Other examples of what has been called 'informational goods' (Lodder and Kaspersen 2002: p. 97) include: copyright and related rights; the protection of data bases; expert systems; (software) patents; trade secrets; trade names and trademarks; service marks; design rights; know-how; domain names; logos; and inventions.

Copyright and related rights play an important role in the information society as they stimulate creation and innovation. According to Recital 2 of the 'Copyright Directive' 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society: "copyrights and related rights protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content".

Within eGovernment, use can be made of several creations of the minds of others. For example, governments can compile information themselves, or engage private third parties within this process. IPR can also be vested in the means of communication, such as in the ICT infrastructure or in software, used by governments to communicate with, or deliver eGovernment services to, citizens or businesses.

2. How is the area IPR related to barriers to eGovernment?

For governments, it is of great importance to assess the implications that intellectual property rights can have with regard to a specific form of electronic communications or form of service delivery in order to avoid liability for a breach of IPR. When disseminating information, governments must pay attention to who owns the information's intellectual property. When publications are made by private parties on the order of public authorities, a government agency needs to be sure that disseminating this information won't be in violation of the intellectual property of the private party. When governments request certain information to be delivered to them by private parties, the question also arises whether the private party can deliver this information to government without violating the rights of others who were responsible for creating the requested information.

To give a real life example: suppose that an archiving agency wants to digitize the complete collection of planning applications for building permits. This agency could make two violations of the law. First, the drawings within the building permits archives are copyright protected. In most cases, the originator of the drawings – often an architect – is the copyright owner. The storage of these drawings in a computer is an unauthorized reproduction, which cannot be compared with copying information for educational purposes or for private use by a natural person. Furthermore, the online distribution of information is also a way of making information available, which is not allowed according to the Copyright Directive.

In applying IPR to software, the following quotation from Välimäki (2005) is of interest: "The owner of intellectual property rights has the exclusive right to prohibit others from using

those rights. Exclusive rights do not pose problems to the software ecosystem as long as the rights can be clearly separated from each other and the creators of new programs are not dependent upon the rights of others. Unfortunately, the implementation of even a simple computer program in the systems that are in use today typically depends on software components from many others. Thus, one company or independent developer can hardly produce a complete software product alone and without the explicit acceptance of others. Understandably, the fragmentation and overlapping of rights pose practical problems as software products become more complex and more parties participate in the development process. The interdependence of rights owners can create difficult lock-in situations if the “difficult” rights owner tries to get as much control through the interfaces of exclusive rights. They may not license the intellectual property at all or may offer only non-acceptable terms. Especially open source developers seem to have a strict criterion that licenses cannot have any royalty requirements.”

Another barrier that could originate out of intellectual property rights lies in the field of patent law. In theory, a patent on parts of a technology that act as gateways, and that therefore need to be interoperable, can be used to block access to new entrants – either by actually prohibiting access or, more likely, by charging licensing fees that are too high (see Harbour and Gentry 2005). In this respect, it may be necessary to establish a strengthened legal mechanism to force owners to open their technology to others if they are unreasonably restricting access.

In general, it is often stated that if the IPR is too strong there will be increasing costs, inefficient centralization, less innovation and, in the end, slower technological progress. All these issues can impede the development of eGovernment.

3. What is the European context for this area, including legislation, policy statements, institutional arrangements relevant to this topic?

Many regulations concerning IPR have already been proposed and implemented to support the establishment and functioning of the internal market within the European Community.³⁶ For example, the following topics have been covered in European Directives:

- enforcement of IPR (Directive 2004/48/EC (and Corrigendum in European Parliament 2004);
- resale right for the benefit of the author of an original work of art (Directive 2001/84/EC);
- copyrights and related rights (Directive 2001/29/EC); protection of data bases;
- term of protection of copyright and related rights (Directive 93/98/EEC); satellite and cable (Directive 93/83/EEC);
- rental right (Directive 92/100/EEC);
- protection of computer programs (Directive 91/250/EEC); and
- semiconductors (Directive 87/54/EEC).
- Actual and proposed legislation concerning industrial property including³⁷:
- patents³⁸;

³⁶ For an overview of the European directives relating to copyrights and neighbouring rights, see: http://europa.eu.int/comm/internal_market/copyright/index_en.htm

³⁷ For full details see the EU Industrial Property website (http://europa.eu.int/comm/internal_market/indprop/index_en.htm).

³⁸ In January 2006, the Directorate General for Internal Market and Services consulted stakeholders on their needs in relation to the legal framework and possible actions in the field of industrial property. Views were sought on the patent system in Europe, and what changes if any are needed to improve innovation and competitiveness, growth and employment in the knowledge-based economy. On July 3, 2006, the preliminary findings from this consultation were published on the European

- trade marks³⁹;
- biotechnological inventions (Directive 98/44/EC);
- designs (Directive 98/71/EC); and
- and the patentability of computer-implemented inventions⁴⁰.

It is important to note that Directive 92/100/EEC has been repealed and replaced by Directive 2006/115/EC, without prejudice to the obligations of the Member States relating to the time-limits for transposition into national law of the Directives. Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property has been substantially amended several times. In the interests of clarity and rationality the said Directive and its amendments have been codified in a consolidated version, Directive 2006/115. This newly updated directive includes⁴¹:

- a harmonization of exclusive rights to authorise or prohibit the rental and lending of works subject to copyright and other objects subject to neighbouring rights;
- a harmonization of certain neighbouring rights including the right of fixation, reproduction, broadcasting and communication to the public and distribution;
- a determination of the beneficiaries of rights related to copyright: performers, phonogram producers, film producers and broadcasters;
- Member States can derogate from the exclusive public lending right, provided that at least authors obtain remuneration for such lending; and
- the principal director is defined to be the author of a cinematography work.

Also, Directive 93/98/EEC has been repealed and replaced by Directive 2006/116/EC, without prejudice to the obligations of the Member States relating to the time-limits for transposition into national law of the Directives, and their application. Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights has been substantially amended. In the interests of clarity and rationality the said Directive and its amendments have been codified in a consolidated version. (Directive 2006/116)

This newly updated directive includes⁴²:

- a total harmonization of the period of protection for each type of work and each related right in the Member States – copyrights expire 70 years after the death of the author of a work and neighbouring rights last 50 years ; and
- harmonization of the period of protection for previously unpublished works, critical and scientific publications, and photographs.

Attention has been given to IPR not only at the European level, but also in a broader international perspective. For instance, the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)⁴³ attempts to narrow the gaps in the way IPR is protected around the world, and to bring them under common

Commission's Industrial Property website

(http://ec.europa.eu/internal_market/indprop/news/index_en.htm).

³⁹ For European Commission and European Council regulations in the field of Trade Mark Law, see:

http://europa.eu.int/comm/internal_market/indprop/tm/index_en.htm

⁴⁰ The 6 July 2005 the European Parliament has rejected the Councils' common position on patentability of Computer Implemented Inventions and the legislative procedure was closed

⁴¹ http://www.law.unimelb.edu.au/ipria/developments_in_ip/intdev/eu.html

⁴² http://www.law.unimelb.edu.au/ipria/developments_in_ip/intdev/eu.html

⁴³ See <http://www.wto.org>

international rules. The agreement lays down a minimum level of protection that each government has to give to the intellectual property of fellow WTO members. It covers:

- copyright and related rights;
- trademarks, including service marks;
- geographical indications;
- industrial designs;
- patents, the European Commission has set out its vision, in the form of a Communication, for improving the patent system in Europe and for revitalizing the debate on this issue. Making the Community patent a reality and improving the existing patent litigation system should, together with supporting measures, make the patent system more accessible and bring cost savings for all;⁴⁴
- layout-designs (topographies) of integrated circuits;
- undisclosed information, including trade secrets.

Other relevant international agreements include two coordinated by the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) (see <http://www.wipo.int>).

The large amount of legal regulation in these areas does not guarantee that all IPR-related barriers to eGovernment have been lifted. There is much academic discussion concerning the future of intellectual property and the need for flexibility within its regulatory systems, as well in discussions on software patents and the threat to open source software. Furthermore, questions regarding the level of harmonization also remain in areas in which Directives have been implemented. These concerns are illustrated here through the following comments on three Directives relating to: copyright; databases; and the re-use of Public Sector information.

3.1 The Copyright Directive (2001/29/EC)

The Copyright Directive (2001/29/EC) has been introduced as an essential building block for the Information Society.⁴⁵ In its Recital 4, the economic importance of harmonization of the European legal framework on copyright has been stressed: “A harmonised legal framework on copyright and related rights, through increased legal certainty and while providing for a high level of protection of intellectual property, will foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness of European industry, both in the area of content provision and information technology and more generally across a wide range of industrial and cultural sectors. This will safeguard employment and encourage new job creation.”

However, a close reading of the Directive, can lead to the conclusion that it does not really harmonize copyright law in the Member States. It leaves the Member States a large bandwidth within which to implement the Directive in their national legislation. For example, Article 5 of the Directive leaves Member States the freedom to provide for exceptions or limitations to the rights provided for in Articles 2 (Reproduction right) and 3 (Right of communication to the public of works and right of making available to the public other subject-matter) for the “use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings.”

⁴⁴<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/463&type=HTML&aged=0&language=EN&guiLanguage=fr>

⁴⁵ The European Commission welcomed the adoption of Directive 2001/29/EC in a Press Release, available at: <http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/01/528&format=HTML&aged=1&language=EN&guiLanguage=en>

As an explanation of this provision, Recital 34 of Directive 2001/29/EC states: “Member States should be given the option of providing for certain exceptions or limitations for cases such as educational and scientific purposes, for the benefit of public institutions such as libraries and archives, for purposes of news reporting, for quotations, for use by people with disabilities, for public security uses and for uses in administrative and judicial proceedings.”

This provision was new to some systems of law. The relevance of the exception for uses in administrative and judicial proceedings is shown by a case in France where a litigant was sentenced for counterfeiting for having read a text under copyright during a plea (Lodder and Kaspersen 2002: pp. 109-10).

3.2 The Database Directive (96/9/EC)

Information in databases is protected by national provisions based on the ‘Database Directive’ (96/9/EC). This harmonizes the copyright protection for databases. According to it, a ‘database’ means a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. Because the database protection is a *sui generis* protection⁴⁶, it differs from copyright protection in that it does not require any form of creativity from the originator. This also means that factual data can be protected on the condition that the data have been assembled in a database and that this activity has required a substantial investment. The contents of a database are protected if the process of obtaining, verifying and presenting the data elements represents a substantial investment in qualitative or quantitative terms (Schellekens 2005).

Even though the Database Directive seemed necessary to enact in 1996, its relevance is now being questioned, as is clear from a recent evaluation by the European Commission (2005b), whose proposed options included repealing the whole directive and another to repeal the *sui generis* right. The evaluation invites stakeholders to provide further evidence on the economic impact of *sui generis* protection in stimulating the production of databases in Europe. It would be wise to reflect on the effect these options might have on existing or future eGovernment communications and services that make use of databases.

3.3 The Re-use Directive (2003/98/EC)

In the European context, it is also relevant to highlight what could be called the ‘commercialization’ of government information. This was regulated from November 2003 in the Directive (2003/98/EC) on the re-use of public sector information⁴⁷. In April 2006, the European Commission also adopted Decision 2006/291/EC Euratom on the re-use of Commission information⁴⁸. According to a report by the HELM Group and Zenc (2006), the estimated overall market size for public sector information in the EU ranges from €10 to €48 billion, with a mean value around €27 billion.

Governments collect much information for their administrative purposes. This is not only of importance for the participation of the citizen in a democratic society, but it also has economic value. For example, government information is the raw material for the

⁴⁶ As explained in European Commission (2005a: p. 19): “The provisions of the Directive protect databases by copyright if they are sufficiently creative (e.g. an encyclopaedia on CD) and/or by the so-called ‘*sui generis*’ right, if substantial financial and professional efforts were involved in their creation (e.g. a telephone directory). The ‘*sui generis*’ right is a specific property right for databases that is unrelated to other forms of protection such as copyright.”

⁴⁷ See also the European Commission’s Public Sector Information website (http://europa.eu.int/information_society/policy/psi/index_en.htm).

⁴⁸ See: Euratom, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_107/l_10720060420en00380041.pdf

information industries to create value added goods and services, such as navigation systems or SMS-services for weather or traffic.

Member States are encouraged by the Directive, but not obliged, to make government information available for re-use for commercial and non-commercial purposes. An exception is made for documents that are copyright protected by third parties. This is explained in Recital 22 of the Directive: "The intellectual property rights of third parties are not affected by this Directive. For the avoidance of doubt, the term 'intellectual property rights' refers to copyright and related rights only (including *sui generis* forms of protection). This Directive does not apply to documents covered by industrial property rights, such as patents, registered designs and trademarks. The Directive does not affect the existence or ownership of intellectual property rights of public sector bodies, nor does it limit the exercise of these rights in any way beyond the boundaries set by this Directive. The obligations imposed by this Directive should apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (the Berne Convention) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement). Public sector bodies should, however, exercise their copyright in a way that facilitates re-use."

Therefore, the Directive is not applicable to documents for which third parties hold intellectual property rights⁴⁹. However, it allows Member States to regulate how administrative bodies make charges for the re-use of government information. The total income from supplying and allowing re-use of documents may not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment.

Furthermore, it is left to the Member States to regulate how public sector bodies may impose conditions for the re-use of public sector information in a licence, dealing with relevant issues.⁵⁰ These relevant issues include: liability; the proper use of documents; guaranteeing non-alteration; and the acknowledgement of source. If public sector bodies license documents for re-use, the licence conditions should be fair and transparent. Standard licences that are available online may also play an important role in this respect. Therefore, Member States should provide for the availability of standard licences⁵¹.

Although the Directive on the re-use of public sector information contributes to the transparency of activities by public sector bodies, it can be concluded that the Directive does not really harmonize the national provisions for such re-use. On several important issues, especially on the principles governing charging, a large degree of flexibility is left to Member States (Janssen 2006:60). For pan-European eGovernment, it is necessary to overcome these national differences, which might only be possible by imposing European standards, either in soft law⁵² or in hard law.

4. What is the relationship of IPR to the seven barrier categories and associated research questions?

4.1 Leadership failures (significant)

As good leadership could result in an appropriate level of attention being given to legal IPR aspects of eGovernment, this area should be considered as a significant element of management leadership. For instance, the municipality of Dordrecht in the Netherlands

⁴⁹ Article 1(2b), Directive 2003/98/EC.

⁵⁰ Article 8, Directive 2003/98/EC.

⁵¹ Recital 17, Directive 2003/98/EC.

⁵² The term 'soft law' refers to quasi-legal instruments which do not have any binding force, or whose binding force is somewhat weaker than the binding force of traditional law, often referred to as 'hard law'. The term initially appeared in the area of international law, but more recently it has been transferred to other branches of law [definition from http://en.wikipedia.org/wiki/Soft_law].

warns users of government information of possible violations of intellectual property rights (see also Section 5.3.4.5 below).

4.2 Financial inhibitors (significant)

The costs of developing, implementing and maintaining ICT systems can be high. In this regard, intellectual property rights can also play an important role in areas we have already mentioned, like IPR for documents, the use of databases and software licenses. Therefore, IPR has financial consequences that could become a serious barrier to eGovernment. In this respect, it is important to determine how the costs of software licenses are affecting investments in eGovernment, and whether these costs leading to a greater use of free open source software⁵³?

4.3 Digital Divides and Choices (significant)

eGovernment resources can be used in different ways, for example depending on social and economic divides. From a social point of view, it can be supposed that the younger generation of consumers are less aware of IPR issues than the older generation and might be influenced by the fact that digital music and movies are freely available on the Internet. This might influence their awareness, or lack of awareness, of IPR issues.

From an economic point of view, eGovernment resources involving information that is protected by IPR (copyright, database protection, portrait right, etc.) could have their availability limited by their costs. In this respect, it is worth examining whether access to copyright protected information could be regulated by Digital Rights Management (DRM) Systems. Furthermore, an agency could be blocked in attempting to digitize its archive of applications for building because the archive is copyright protected for the originator and so the storage on computers will be an unauthorized reproduction and the online distribution of such information will not be permitted under the Copyright Directive.

These are examples of possible IPR restrictions that could be influential barriers in this area if plans are not implemented to avoid or eliminate such blockages.

4.4 Poor coordination (significant)

Coordination and harmonization are important issues for appropriate eGovernment networks and services. As discussed above, the relevance of the Database Directive has been questioned in its evaluation. Furthermore, the Directive on the re-use of public sector information is not harmonizing effectively and seems to leave too much bandwidth for the Member States. Dumortier et al (2003: p. 9) claim that Directive (1999/93/EC) on eSignatures seems to require “a primary need for a consistent, clear and workable re-interpretation of the provisions of the Directive.”

Therefore it seems relevant to continue to explore how provisions in Directives that could hinder the effectiveness of administration activity at different levels or become a barrier for the competitiveness of the European economy – and how they can be altered to remove the obstacles that could arise from them.

⁵³ See: <http://www.flossworld.org> for information on the MODINIS initiative Free/Libre/Open Source Software.

4.5 Workplace and organizational inflexibility (significant)

The example in Section 5.3.2 of an agency archiving planning documents shows that there is uncertainty about how to deal with database protection and architect copyrights covering drawings in the database, as also shown by the way users of such information in Dordrecht are warned that architect drawings are copyright protected (see Section 5.3.4.1). However, not all similar projects inform their users about such legal issues. Dealing with such legal issues could become an administrative burden for public administration management and staff. They should therefore be well informed about these and other legal issues in order to be able to share their government information and documents in a legitimate way.

Because employment laws could inhibit flexibility in changing working practices or the deployment of staff, it is relevant to deal with the question of the ways in which the current structure of Employment Law in Member States act as a blockage or facilitator for the restructuring of the public sector labour market that may be needed to realize the full benefits of high levels of ePublic Services delivery and use.

4.6 Lack of trust (significant)

Trust is an important key element for the success of eGovernment. This means, for example, that citizens should not have a 'Big Brother' fear of government monitoring and intrusion in their lives. They must be able to rely on the security within eGovernment services. From an IPR-perspective, it seems important that citizens can rely on the legal compliance of governments with IPR when delivering their eGovernment services.

Public administrations will also have to pay attention to other IPR-issues than database protection. For example, to prevent liability difficulties, and thus enhance trust, the information and documents that are available in eGovernment services should of course be in compliance with other intellectual property rights.

4.7 Poor technical design (significant)

eGovernment services will often be developed using software that is copyright protected. This could create difficulties regarding the use of such exclusive software rights if they are based on licences implementing very inconvenient terms and conditions. On the one hand, using standard software can of course contribute to the standardization between eGovernment networks and services. On the other hand, using standard software can also have important potentially negative consequences in technical (e.g. interoperability obstacles) and financial (e.g. high costs of a commercial software package) areas. Therefore, it is worthwhile to consider the use of open source software for eGovernment services,

In this respect, the way the open source movement is affecting interoperability is discussed below in Section 5.3.5.2. For instance, open source could also constrain interoperability by offering only strict terms on licences that may not have royalty requirements (Välimäki 2005), which means other participants are not incentivized to comply with interoperability requirements. On the other hand, open source software could facilitate interoperability by removing problems caused by complex fragmentation and overlapping of IPR and copyright issues associated with individual software components of an eGovernment application.

5. What are the barriers remaining in this field?

5.1 Infringements of IPR by governments

Private parties can contribute to eGovernment by generating publications and other information for eGovernment services or by providing the ICT infrastructure or software needed to deliver certain electronic services. If the intellectual property rights relating to a publication, infrastructure or software are not transferred to the government, their use by government can lead to IPR infringements. This can lead to another field of law, namely that of liability. Thus, if government makes use of private parties to create information or technological devices to perform eGovernment services, it needs to be sure that disseminating this information or the use of these devices won't be in violation of the intellectual property rights of the private party. IPR infringements by governments could therefore be a significant eGovernment barrier.

The 'active delivery' of public sector information can stimulate demand for eGovernment by making government information readily available to citizens and business. However, publication of government information on a website represents a copyright-protected publication. For example, according to Article 15b of the Dutch Copyright Act: "The further communication to the public or reproduction of a literary, scientific or artistic work communicated to the public by or on behalf of the public authorities shall not be deemed an infringement of the copyright in such a work, unless the copyright has been explicitly reserved, either in a general manner by law, decree or ordinance, or in a specific case by a notice on the work itself or at the communication to the public. Even if no such reservation has been made, the author shall retain the exclusive right to have it appear in the form of a collection his works which have been communicated to the public by or on behalf of the public authorities."⁵⁴

This means that the information published by an administrative body can be used freely, unless the administrative body has made a reservation. To prevent third parties from using copyright-protected government information, the administrative body can make an explicit reservation. Furthermore, the administrative body could also make financial conditions for the further use of copyright-protected government information. An administrative body needs the consent of the originator for the active delivery of the information. When information is published without the originator's consent, and without the reservation mentioned above, the copyright of the originator has been released. The originator can no longer object to the further use of the information made available by the administrative body. However, he can claim compensation from the administrative body for violation of his copyright (Bergfeld, Kaspersen and Lodder 2000). The potential blockages to eGovernment posed by such consideration can be addressed through strong leadership that makes appropriate IPR arrangements and effective coordination between all stakeholders.

A practical barrier arises when the originator of the information does not give consent to the administrative body to publish the information. To prevent this, it might be necessary to adapt the Copyright Acts in the EU Member States. The adaptation of the European copyright law could, for example, create a legal basis for the publication of copyright-protected information by administrative bodies, or create an entitlement to financial compensation.

Another problem on the supply side can come into being with regard to authority over the eGovernment service. When government cooperates with private parties – in whatever legal structure – it is of great importance that government makes the appropriate agreements regarding emerging intellectual property rights. A related issue is outsourced public sector services, where private parties directly assist governments to achieve their public service objectives. However, if the private party owns the emerging IPR, the

⁵⁴ See : <http://www.ivir.nl/legislation/nl/copyrightact.html>

government's influence in developing and exploiting the eGovernment service might be limited and can lead to financial burdens, creating a potential financial inhibitor. To minimize this risk, it might be best if the public sector is at least an equal investor in the IPR relating to, and emerging out of, eGovernment services.

European legislation should be adapted to help further harmonization of European copyright law, and to prevent legal barriers in cases when originators of information refuse to give their consent for publication of information by an administrative body. A general legal basis could be created for European governments to publish government information, or to entitle financial compensation for the copyright owner. Therefore, this barrier can be considered a very significant concern that can only be overcome by a moderation of the European legislation.

Related barriers: leadership failures, financial inhibitors, poor coordination.

5.2 Uncertainty about open standards and open source software

An IPR barrier to eGovernment is an uncertainty within the European patent regime which could pose a threat to open standards as well as open source software.

In the eEurope Action Plan 2005, the European Commission (2005c) states: "an agreed interoperability framework to support the delivery of pan-European eGovernment services to citizens and enterprises" would be issued and that the framework "will be based on open standards and encourage the use of open source software". Such open standards are publicly available specifications that describe the characteristics of a technology with the aim of promoting technical interoperability.

The European Interoperability Framework (EIF) Working Document (IDABC 2004: p. 9) argues that, to reach such interoperability in the context of pan-European eGovernment services, guidance needs to focus on so-called 'open standards'. This document sums up a number of minimal characteristics that a specification and its attendant documents must have in order to be considered an open standard. Based on these characteristics, the Dutch Programme for Open Standards and Open Source Software in Government⁵⁵ (OSSOS 2004, p. 2) defined 'open source' as a standard satisfying the following requirements:

- the costs for the use of the standard are low and are not an obstacle to access it;
- the standard has been published;
- the standard is adopted on the basis of an open decision-making procedure (consensus or majority decision, etc);
- the intellectual property rights to the standard are vested in a non-profit organization, which operates a completely free access policy;
- there are no constraints on the re-use of the standard.

This definition has been criticized, for example by Lueders (2005: p. 11): "When further defining 'open standard', the impact of any 'open standard' definition should be carefully assessed, taking into account the inherent interoperability logic. Moreover, when defining the term 'open standard', the EU should take into account the legal limits to any 'open standard' definition as delineated by public procurement and intellectual property law."

Simply defined, the required form of interoperability is the ability of two or more ICT assets (hardware devices, communications devices, or software components) to easily or automatically work together and to expand to include the ability of two or more business processes or services to similarly work together smoothly. It is clear that this ability to

⁵⁵ See: <http://www.ossos.nl/index.jsp>

interoperate is a key to reducing ICT integration costs and inefficiencies, increasing business agility and enabling the adoption of new and emerging technologies (Lueders 2005). However, if the technologies to realize interoperability are patentable, and high fees are asked to use them, the positive effects of interoperability will certainly be reduced..

Open source software offers the underlying programming code to users so that they may read it, make changes to it and build new versions of the software incorporating their changes. There are many types of open source software, mainly differing in the licensing terms under which (altered) copies of the source code may (or must be) redistributed. Usually, a 'perpetuity clause' is used, stating that further improvements of the software will also be free (open source) software.

The difference between a copyright claim regarding software and a patent claim is related to the scope of the protection. Copyrights rest only on the written program (or code). A software patent relates to the invention and therefore is much broader. The European Parliament turned down a Software Patent Directive proposal in July 2005. This means the legal situation regarding the patentability of computer-implemented inventions remains unclear. The European Patent Office has granted thousands of software patents that may cover interoperability information. However, it is not clear whether those patents are truly valid.

To provide some legal certainty, and to prevent open standards and open source becoming eGovernment barriers, more clarity is needed on: what can and what can't be patented; what exactly the definition is of interoperability; and if, how and when regulators can impose a requirement on a patent holder to grant a licence to open their technology to others.⁵⁶ Overcoming this barrier therefore requires good leadership and effective coordination.

For the ICT industry at large, reasonably priced interoperability licence fees do not create barriers. However, many open source advocates, academics and some small companies argue that such standards essentially close interoperability information for those who cannot meet the criteria in the licences.

The previously mentioned uncertainties regarding patentability and open source software are not the only bottlenecks that can be created by the use of open source software in eGovernment. As a survey in the Netherlands found: "Nevertheless, 70% of the interviewed government officials indicated that they thought the dependence on proprietary software companies to be too big. A survey of the use of open source software by educational institutions showed that open source software is being used, although the percentages are still low. Many educational institutions indicated that they needed more information about open source. The unfamiliarity with open source software is thus still a bottleneck. Sometimes the non-use of open source software by government can be traced back to trivialities. For instance, the requirements that the government sets for calls for tenders for software projects appear to discriminate against open source companies. Requirements of annual turnover and company size are set so high that many open source companies fall by the wayside. The Minister has promised to re-evaluate government policy with respect to tenders."⁵⁷

The open source debate is also relevant to the development of eGovernment in poor nations. They won't be able to solve their development problems unless they stop having to pay high software licensing fees.

Related barriers: leadership failures, financial inhibitors, digital divides and choices, poor coordination.

⁵⁶ Article 31 of TRIPS gives some guidance in this respect.

⁵⁷ Quotation from an interview held with Maurice Schellekens, an expert in national and international Intellectual Property Rights.

5.3 Interoperability of technical systems

Blockages caused by the poor interoperability of technical systems can be an important eGovernment barrier. For instance, if only one computer system or software package can be used to access an eGovernment service, citizens and businesses using different systems or software will simply be deprived of that service.

eGovernment should therefore not be based on one specific standard, technology or platform that users are obliged to employ to engage with available services. Instead, enterprises and citizens should be able to choose between different suppliers of software that could help them to use the services of public authorities. As an example, from 2006 the Dutch electronic tax form has been available for Apple and Linux platforms. Before then, only users of Microsoft Windows platforms were able to take advantage this service. From the viewpoint of government, providing such a range of options is essential to the availability and cost-effectiveness of the service. A competitive strategy can ensure the presence of different products and lead to better and cheaper services. A condition that must be met for this to be achieved is that open standards are used and compatibility problems between different formats are solved.

The following quotation from Välimäki (2005: p. 3) illustrates the related issues of whether only one or more technologies can be used, and the way that is closely related to discussions about the patentability of software: "Many technology companies would like to see their proprietary software technology become standard and then control the surrounding 'ecosystem'. To contrast, interoperable developers and the users of technology at large would like to see all standards to have open non-proprietary interfaces without any intellectual property protection...European copyright laws have a well-established principle that a single right owner can't control interoperability information through copyright [Article 6, Directive 91/250/EEC]. Unfortunately patent law does not know such exception: it must be therefore balanced through alternative means."

European legislation that promotes the use of multiple open standards, technologies or platforms could be a significant means of improving eGovernment interoperability and in clearing uncertainties regarding the patent system.

Related barriers: financial inhibitors, digital divides and choices, poor coordination, poor technical design.

5.4 Infringements of intellectual property rights by governments

When government requests certain information to be delivered to them by private parties, the question arises whether the private party can deliver it without violating the rights of those who created the requested information.

A private party who delivers copyright protected information from another party to the government is liable for violating these copyrights. For instance, to apply for a building permit, citizens or other organizations often have to deliver copyright-protected drawings originated by certain architects based on a specific client's clear instructions and ideas. This means that nobody is allowed to use these drawings for building purposes or to distribute or copy them unless consent has been given by the architect who holds the drawings' copyright. The architect can transfer the copyright, for example under the condition that the drawings may not be changed or may be used only once. The architect can also ask for financial compensation.

It is questionable whether governments at national and European level can claim that they are not accountable for violating IPR in the same way as private parties. More investigation is needed into whether governments should have an obligation to notify the owner of a copyright before delivering his or her information to the government. Arrangements may

have to be made with the receiving government, which could be obliged to make the information available to third parties.

For passive, rather than active, delivery of public sector information, it does not seem justified for an administrative body to use a plea of copyright protection to refuse a request based on a Freedom of Information (FOI) Act. However the receiver of the information does not have a right to free disposition of the information and needs the consent of the administrative body for copyright-related acts. It is also questionable whether an administrative body is obliged to highlight such use limitations. For instance, the Dutch Copyright Act does not oblige the administrative body to do so, although it seems to be a sensible course of action.

In this respect, we can point at the Building Archives of the Dutch municipality of Dordrecht. In its department of Building and Living (Bouwen en Wonen), an archive of data relating to homes and other buildings in the municipality is kept up to date. This contains building permits, demolition permits, building drawings, construction calculations and construction drawings. Anyone can have access to this archive, and can take a copy of one or more of these archived documents, at a reasonable cost and with tips and points of interests mentioned on its website⁵⁸. One clarification about copyright-protected warns: "In the archive, a lot of granted building permits are being retained. As is stated before, you can use these documents for example for your application. We urgently call for your attention that building drawings, construction drawings, and construction calculations are copyright protected. To make use of these documents, you need the consent of the copyright owner. You are responsible yourself for obtaining consent."

A warning like this can be considered an obligation for government, based on administrative carefulness and requires careful thought about the technical design of the user interface to information. A lack of coordination among stakeholders in this field could also put a brake on the eGovernment service.

To address this, it doesn't seem necessary to change the legislation with regard to IPR, although some specific legal points of interest have been highlighted. It should be noticed that a warning to the user of government information seems necessary from the perspective of fair administration.

Related barriers: poor coordination, poor technical design.

Sources

Publications

European Commission (2005a), 'Evaluation of the 1996 Database Directive Raises Questions', Brussels; European Commission, DG Internal Market and Services in December, http://europa.eu.int/comm/internal_market/smn/smn40/docs/database-dir_en.pdf

European Commission (2005b), First Evaluation of Directive 96/9/EC on the Legal Protection of Databases, DG Internal Market and Services Working Paper, Brussels: European Communities, DG Internal Market and Services Working Paper, 12 December, http://europa.eu.int/comm/internal_market/copyright/docs/databases/evaluation_report_en.pdf

European Commission (2005c), eEurope 2005 Action Plan, Communication to the Council, the European Parliament, the European Economic and Social Committee and The Committee of the Regions, Brussels: European Commission,

⁵⁸ See:

http://www.dordrecht.nl/pls/idad/prodEgemProductToon?F_PRODUCTID=999920021209131220

http://europa.eu.int/information_society/eeurope/2005/all_about/action_plan/index_en.htm

- European Parliament (2004), Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of Intellectual Property Rights, Official Journal of the European Communities L 195, 2 June, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_195/l_19520040602en00160025.pdf
- Harbour, M. and Gentry, S. (2005), 'Intellectual Property and the Challenge of Digital Technology', European Review of Political Technologies, 3, December 2005, pp. 1-5. http://www.politech-institute.org/review/articles/HARBOUR_Malcolm_&_GENTRY_Simon_volume_3.pdf
- HELM Group and Zenc (2006), Study on Exploitation of Public Sector Information Benchmarking of EU Framework Conditions: MEPSIR – Measuring European Public Sector Resources, June, Moira, Northern Ireland, UK: HELM Group of Companies and The Hague: Zenc, available at the European Commission's Public Sector Information Benchmarking Study's website: http://europa.eu.int/information_society/policy/psi/psi_benchmarking_study/index_en.htm
- IDABC (2004), European Interoperability Framework For Pan-European eGovernment Services, Luxembourg: Office for Official Publications of the European Communities, <http://ec.europa.eu/idabc/servlets/Doc?id=19529>
- Janssen, K. (2006), 'Hergebruik van Overheidsinformatie – Binnenkort ook bij u in de Winkel?', *Privacy & Informatie*, 9, pp. 59-64.
- Lueders, H. (2005), 'Intellectual Property Rights and eGovernment Interoperability in Europe', European Review of Political Technologies, 3, December, pp. 1-13. http://www.politech-institute.org/review/articles/LUEDERS_Hugo_volume_3.pdf
- Schellekens, M. M. H. (2005), 'Intellectual Property Issues Relevant for the European Transport Information System', in Giorgi, L., Klautzer, L., Rahman, A. and Schmidt, M. (eds.), *Towards a European Transport Policy Information System*, ETIS-LINK.
- OSSOS (2004), Stichting ICTU, Programma OSSOS: Programme For Open Standards And Open Source Software in Government, <http://www.ossos.nl/index.jsp?alias=english>
- Välimäki, M. (2005), 'Software Interoperability and Intellectual Property Policy in Europe', European Review of Political Technologies, 3, December, pp. 1-11. http://www.politech-institute.org/review/articles/VALIMAKI_Mikko_volume_3.pdf
- International and European-level Legislation, Regulations, Conventions and Treaties
- Note that an overview of European Directives relating to copyrights and neighbouring rights is provided at:* http://europa.eu.int/comm/internal_market/copyright/index_en.htm
- Commission Decision of 7 April 2006 on the re-use of Commission information, 2006/291/EC, Euratom, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_107/l_10720060420en00380041.pdf
- Directive 2001/29/EC of 22 May 2001 of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights in the information society, Official Journal of the European Communities L 167, 22/06/2001, pp. 10-19, http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_167/l_16720010622en00100019.pdf
- Directive 2001/84/EC of 27 December 2001 of the European Parliament and of the Council on the resale right for the benefit of the author of an original work of art, Official Journal of the European Communities L 13/10/2001, pp. 32-6, http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_272/l_27220011013en00320036.pdf

- Directive 2003/98/EC of 17 November 2003 on the Re-use of Public Sector Information, Official Journal of the European Union, L 345, 22/06/2001, pp. 90-6, http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_345/l_34520031231en00900096.pdf
- Directive 2004/48/EC of 29 April 2004 of the European Parliament and of the Council on the enforcement of intellectual property rights, Official Journal of the European Union, 30/4/2004, L 157, pp. 45-86, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_157/l_15720040430en00450086.pdf (see also Corrigendum in European Parliament 2004)
- Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, Official Journal of the European Communities L 024, 27/01/1987, pp. 36-40, <http://europa.eu/scadplus/leg/en/lvb/l26025.htm>
- Directive 91/250/EEC on the protection of computer programs of 14 May 1991, Official Journal of the European Communities, L 122, 17/05/1991, pp. 42-6
- Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, Official Journal of the European Communities L 346, 27/11/1992, pp. 61-6, http://europa.eu.int/ISPO/ecommerce/legal/documents/392L0100/392L0100_EN.doc
- Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, Official Journal of the European Communities L 290, 24/11/1993, pp. 9-13, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:EN:HTML>
- Directive 96/9/EC of 11 March 1996 of the European Parliament and of the Council on the legal protection of databases, Official Journal of the European Communities L 077, 27/03/1996, pp. 20-8, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=E&numdoc=31996L0009&model=guichett
- Directive 98/44/EC of 6 July 1998 on the legal protection of biotechnological inventions, Official Journal of the European Communities L 213, 30/07/1998, pp. 13-21, http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_213/l_21319980730en00130021.pdf
- Directive 98/71/EC of 13 October 1998 on the legal protection of designs, Official Journal of the European Communities L 289, 28/10/1998, pp. 28-35, http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_289/l_28919981028en00280033.pdf
- Trade Mark Law regulations in the EU are provided at:
http://europa.eu.int/comm/internal_market/indprop/tm/index_en.htm

Websites

- European Commission, Industrial Property website providing information on actual and proposed legislation concerning IPR
(http://europa.eu.int/comm/internal_market/indprop/index_en.htm)
- European Commission, Public Sector Information website
(http://europa.eu.int/information_society/policy/psi/index_en.htm)
- IDABC, Open Source Observatory, dedicated to Free/Libre/Open Source Software with the aim of encouraging the spread and use of best practices in Europe
(<http://ec.europa.eu/idabc/en/chapter/5883>)
- European Interoperability Framework documentation
(<http://europa.eu.int/idabc/en/document/3473/5585>)
- World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (<http://www.wto.org>)

eGovernment barriers: deliverable report 1b

World Intellectual Property Organization (WIPO) Copyright Treaty (WCT) and Performances and Phonograms Treaty (WPPT) (<http://www.wipo.int>)

Research projects

Information Society Activities at a Glance

(http://europa.eu.int/information_society/activities/index_en.htm)

Free/Libre/Open Source Software (<http://www.flossworld.org>)

Paper 4: Liability and eGovernment

Dr Collette Cuijpers

Tilburg Institute for Law, Technology, and Society (TILT), University of Tilburg, Netherlands

1. Description of the Area

eGovernment is not a one way street. Its purpose is not only to disseminate information from the administration to the public or to facilitate or enhance public services; it is also about information relationships between government, businesses and civilians. These relationships work both ways, in that two-way electronic access to basic administrative interactions, interactive communication and feedback on political initiatives are as important as one-to-many information and service delivery from a public body. An optimal functioning of eGovernment can therefore be described as involving four processes:

- information delivery;
- communication between public bodies and citizens/companies;
- transactions between the above partners;
- interaction and participation.

Within all these processes, there is a need for a division of responsibility regarding damages resulting from a malfunction in the process or from inaccuracies in the information being processed. Black's (2004 [1891] Law Dictionary, for example, defines liability law as: "Legal responsibility to another or to society, enforceable by civil remedy or criminal punishment".⁵⁹ The division of liability within eGovernment processes needs to be dealt with on the basis of general tort law and contracts, governed by general contract law. With regard to the contractual relationship, the law provides several mechanisms to deviate from the general rule that everybody is responsible for their own actions. Limitation and even exclusion of liability is possible, although only to a legally limited extent. The special role government plays within society can give reason to interpret very strictly the boundaries of limitations or exclusion of liability in the public sector, which raises the possibility of insuring liability risks. Liability is most often seen as a manageable blockage to eGovernment as it leaves room for alternative scenarios when seeking responses to a challenge.

This section discusses why liability law is not in itself a real barrier to eGovernment, but is essentially a mechanism to allocate legal responsibilities as a means of removing blockages to eGovernment progress. In specific situations, dependent on many variables in particular contexts, these responsibilities can lead to great financial risks in relation to both eGovernment supply and demand. Thus, each and every eGovernment initiative requires its own cost/benefit analysis. This should be drawn on when making decisions about whether to proceed with an eGovernment initiative or to await on certain kinds of legal or other adaptations to become available to reduce the liability risks. The outcome of a cost/benefit analysis should lead to answers on whether or not a barrier to an already-initiated eGovernment process exists and its implications on the further development or impairment of this eGovernment initiative. Indications of which legislative or other measures need to be taken to lift a barrier should also flow from this analysis.

Even if this analysis shows that it might not be wise to proceed with the eGovernment initiative under the present conditions, the initiating government is still free to decide that the risk is acceptable in the circumstances. The need to assess liability risks specifically for

⁵⁹ Blacks' law dictionary 2004.

every eGovernment service further indicates why liability is not in general a barrier as such, although it can be a significant factor within key barriers. As discussed below, adopting approaches like the Principles of European Contract Law would create more legal certainty and decrease the likelihood that liability law, and the fear of being liable, contribute to the formation of barriers to eGovernment.

2. How is the area of Liability related to the barriers to eGovernment?

In electronic communications, all kinds of scenarios can be sketched regarding questions of liability. Messages or services can reach recipients too late, not at all or can be delivered to the wrong recipients. With regard to the contents, there can be inaccuracies or infringements of a law such as that relating to copyrights or privacy. These examples show that there is not always a distinct difference between electronic and non-electronic communication, in which the same errors can occur. However, in electronic communication: the risks of a malfunction might be higher; the effect of the malfunction could lead to much greater damages; and it might be harder to ascertain and prove where responsibility for the malfunction lies.⁶⁰ This can, for example, be the result of an information aggregation process, where it might be hard to ascertain which source, or which combination of sources, lead to inaccuracies in the information. A further problem can be the traceability of malignant third parties interfering in the eGovernment process.

Another reason for barriers to eGovernment arising within the field of liability is the different legal approach taken regarding contractual and non-contractual liability throughout the EU. This point is of even greater importance with regard to electronic communications, as often the circle of parties involved in delivering the communication or the service is larger than in non-electronic communication. A simple example is communication by means of a letter, as opposed to the sending of an email. With the delivery of the letter, only government, the post company and the recipient are concerned. With the delivery of an email, the government probably needs to make use of an access provider, as well as a service provider. The same holds true for the recipient. The eGovernment process also involves software and hardware used by government and users to send and receive emails within which malfunction could also influence the electronic communication. This simple example shows that in electronic communication, and probably even more in electronic service delivery, the contractual relations might be more complex when using traditional means.

In relation to the content of information, there is not that much difference between electronic and non-electronic communication. A government official can as easily make errors in a letter as in an email. The question of whether or not it is easier for a third party to alter an electronic message or a traditionally written message is hard to answer in general, as it depends to a large extent on the security measures taken. In this respect, a direct link can be made to our paper on Authentication and Identification (Section 5.2).⁶¹ As already mentioned, the simple aggregation of information in an online environment could lead to a higher number of inaccuracies in the information being processed. On the other hand, ICT can easily be used to detect inaccuracies, to prevent inaccuracies from coming into being or to correct inaccuracies. To be able to come to a conclusion in this respect, empirical research is needed to ascertain whether or not, and under what circumstances, electronic information processing is more likely to generate inaccuracies than non-electronic information processing. The much greater ability to aggregate and integrate content and services from different organizations, in both the public and private sectors, can also lead to inaccuracies in the content through: a possible lack of visibility of the source of the problem; difficulty in proving causation; and the possibility of large scale damage in an electronic environment.

⁶⁰ See, for example, NECCC (2000: 39), a guidebook that recommends governments should consider establishing a legal framework that treats electronic processes and traditional processes equally.

⁶¹ Georges Chatillon (2002) remarks that advancing eGovernment requires identification and authentication procedures that do not render public authorities liable.

Another link can be made to privacy and data protection, as the aggregation and integration of information can lead to severe infringements resulting in liability risks.⁶² All these circumstances could inhibit moves to change from non-electronic to electronic means of communication and service delivery, as well as to the development of new electronic services. For instance, the introduction of a Dutch National Electronic Patient Record⁶³ was postponed because the gaining of unauthorized access by a hacker made it obvious that the level of security of the information within these records was not sufficient, which led to a perception among hospital managers of high liability that meant they naturally refused to take up this innovation.

In this respect, addressing eGovernment at pan-European level might increase liability risks as the complicated technical structure as well as the lack of uniformity within the legal framework could cloud assessments of predictability and therefore makes liability assessment difficult.

3. What is the European context for this area?

Liability is an issue that needs to be addressed for all government actions. The risks for legal liability, which result in financial responsibilities, need to be assessed for every form of interaction between government and citizens or businesses. As mentioned above, risks in an electronic environment can be different, especially with regard to the ease of cross-border activities within this environment. Government services are often confined to territorial borders, which simplifies and restricts the risks of liability. With pan-European eGovernment services, the crossing of borders is a fundamental concept. This leads to a much more complicated legal framework regarding liability.

In the EU, there is no unified general law on contractual or non-contractual liability. Several projects are, or have been, run with the aim of harmonizing tort law, the law on contract – and even the development of a ‘European Civil Code’.⁶⁴ None of these projects has so far led to legally binding regulations.⁶⁵ However, it is possible to conceive of harmonized rules regarding liability issues within the EU. For example, several specific European Directives include clauses regarding liability in specific areas or concerning specific parties:

- the eCommerce Directive (2000/31/EC)⁶⁶ contains provisions regarding liability of intermediary service providers;
- Directives 1999/34/EC⁶⁷ and 85/374/EEC⁶⁸ concern product liability;

⁶² Privacy and data protection is used as an example to plead for establishing an eGovernment no-fault liability. As Chatillon (2002) notes: “The inevitable risk in electronic data processing resurrects the theory of no-fault liability and gives rise to a variation in liability for an error caused by information technology”. He also points out that it would be reasonable to adopt a principle of precaution taking into account the risk in electronic data processing.

⁶³ See Markenstein (2005), Michel-Verkerke, M. B. and Spil, T. A. M. (2002) and the websites: <http://www.minvws.nl/dossiers/elektronisch-patienten-dossier/> or <http://events.ccc.de/congress/2005/fahrplan/events/489.en.html>

⁶⁴ See for example von Bar and Drobnič (2003) and von Bar, Lando, and Swann (2002).

⁶⁵ Even though the Principles of European Contract Law (PECL) do not have the authority of national, supranational or international law, this does not mean they have no legal relevance. A choice of law for the Principles can be made in case of an international contractual relationship in order to overcome differences in national legislation. The choice for the PECL can be to avoid difficulties in agreeing on a national system of law. If no explicit choice of law is made in a contractual international relationship, the courts might apply the PECL. The justification for applying the Principles is that it is hoped that they will furnish a more appropriate basis than any system of national contract law for the adjudication of an international contract (see Busch 1998).

⁶⁶ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML>

⁶⁷ Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, <http://eur->

- the eSignature Directive (1999/93/EC) refers to national liability rules but does require a minimum level of liability⁶⁹; and
- the unfair contract terms Directive 93/13/EEC⁷⁰ limits the validity of contract terms that exclude liability.

Furthermore, in several fields of law in which Directives have been adopted, there are provisions as to who will be liable for breaching the law under particular circumstances. Directives relating to database protection and privacy⁷¹ are also of relevance in this respect. Even though these regulations bring some clarity to specific legal relationships, they do not constitute a harmonized legal framework regarding liability. The level of harmonization established by these Directives is also typically ambiguous,⁷² as differences remain in interpretations of their provisions and in national legal implementations.⁷³

Without a European legal framework, liability for eGovernment is to a large extent therefore regulated by national law. Research undertaken on the harmonization of European law in this area has clearly revealed that within the EU a legal 'rift' exists in liability law. For instance, many differences exist between contractual and non-contractual liability covering a large variety of legal rules not only between Common Law countries (e.g. UK) and Civil Law countries (e.g. France, Germany)⁷⁴, but also between different Civil Law regimes. Research⁷⁵ regarding European Private Law that is seeking to answer the question of whether this rift should be solved by European legislative measures has so far indicated that the differences in the liability regimes lead to barriers to enter the European Market.⁷⁶ The arguments behind this conclusion can also be used with regard to the question of

lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31999L0034&model=guichett

⁶⁸ Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31999L0034&model=guichett

⁶⁹ Article 6 of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 13, 19/01/2000 P. 0012 -0020, http://europa.eu.int/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf

⁷⁰ Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:EN:HTML>

⁷¹ Directive 96/9/EC of 11 March 1996 on the legal protection of databases, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31996L0009&model=guichett; Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_2011_l_20120020731en00370047.pdf; and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

⁷² For example, the evaluation of the e-Commerce directive shows a difference in scope of the articles concerning service provider liability. Spain and Portugal have, in addition to the matters dealt with by Articles 12-14, decided to provide for limitations on the liability of providers of hyperlinks and search engines (see European Commission 2003a).

⁷³ See for example the reports on the transposition and operation of directives covering data protection, electronic signatures and defective products (European Commission 2003b; 2006a; 2006b).

⁷⁴ For instance, for more on Tort Law, see the European Group on Tort Law (2005) and for more on Contract Law see von Bar, Lando, and Swann (2002).

⁷⁵ There are at least two groups doing research in this area: the European Group on Tort Law (<http://www.egtl.org>) and the Lando Commission (<http://www.jus.uio.no/lm/eu.principles.lando.commission/>).

⁷⁶ For example, von Bar, Lando, and Swann (2002: 238) note: "Divergent contract law makes it at present impossible to engage effectively in the European market on an informed basis. Businesses which nonetheless dare to take that step are often burdened by costs which are either superfluous or unforeseeable. Risks of liability are extraordinarily difficult to gauge; often they are simply absorbed and may make business unprofitable or loss-making."

whether the differences in liability regulations throughout the EU can be defined as a remaining barrier to eGovernment.

The question as to whether liability law impedes eGovernment is hard to answer in general. Even though the outcome of the research in the field of European Private Law points to the necessity of harmonizing European liability law, this does not mean that every eGovernment initiative is hampered by a lack of harmonization. For example, purely national initiatives will in principle not be affected by differences in national liability laws. However, pan-European initiatives in which many different parties from a lot of different Member States participate may not be pursuable because of the high, or unclear, risks for liability resulting from the differences in national liability laws.

For instance, a study of European Contract Law⁷⁷ outlines the difficulties in confronting businesses and consumers in ascertaining foreign private law and the economic ramifications of legal diversity for the EU internal market. The various European contract laws on non-performance or defective performance are based at present on fundamentally different regimes: either a system of strict liability or a system of fault-based liability. Just as substantial are the differences in the law on validity of penalty clauses and limitation of actions. Disclaimers can be mentioned as an example of uncertainty in this respect, even within national borders. For example, in the Netherlands the status of disclaimers is still unclear. The Dutch Information Office, which is concerned with eGovernment services, states in its legal Frequently Asked Questions that disclaimers cannot be used by government because of its duty of care and the General Principles of Good Administration. Moreover, as verbal promises can already be binding upon government, the same holds true for an email.

It is obvious that different views in respect of the value of such disclaimers leads to great legal uncertainty, not only with regard to government but also in general, as private parties can be involved in eGovernment. In turn, legal uncertainty is a barrier to eGovernment, as liability risks are unclear. This can lead to a lack of trust in the eGovernment service and, therefore, reluctance to switch from traditional to electronic means of service delivery in terms of both the demand and supply sides of eGovernment.

In the above mentioned research regarding European Contract Law, it has also been concluded that neither the mechanism of choice of law nor the freedom to frame contracts enables parties to avoid substantial costs arising out of the real or supposed diversity of the law in the EU. Already the anxiety that differences in other legal systems might result in different legal outcomes leads to a considerable expenditure or effort to obtain very specific legal information and opinion, which in the end may turn out to have been unnecessary. Mention is made of the unnecessarily high premiums for liability insurance because of the very different liability regimes with regard to cabotage⁷⁸ transport, an area that is even already dominated by international conventions.⁷⁹ Even though these research results cannot support the conclusion that in general harmonization of liability law is essential to avoid impeding eGovernment, they do not mean that an ongoing effort to harmonize contractual and non-contractual liability would in general be beneficial to the development of not only eGovernment but also eCommerce. In this respect, the recommendation of Von Bar and Lando to carry out further work in formulating Principles of European Patrimonial Law, both for the sake of soft law and as a pre-requisite for possible future legislation, is specifically interesting to pursue with regard to eGovernment.⁸⁰

4. What is the relationship of liability to the seven barrier categories?

The discussion above indicates that liability is most closely related to the barrier categories financial inhibitors and lack of trust, with poor coordination being particularly important in

⁷⁷ von Bar, Lando and Swann (2002: 183 and 238).

⁷⁸ Cabotage is the transport of goods or passengers between two points in the same country.

⁷⁹ von Bar, Lando, and Swann (2002: 183, 197, 202 and 203).

⁸⁰ von Bar, Lando, and Swann (2002: 183).

relation to the frequent lack of harmonization of legislation. It also explains why every eGovernment initiative it should investigate whether the move from traditional public service delivery methods to electronic methods leads to other, higher, liability risks.

This raises a number of important eGovernment management, system design, implementation, use and research questions systems, such as: What are the relevant differences that influence liability risk? Does the electronic environment and the novelty of electronic service delivery complicate the assessment of risks, and if so in what ways? Does this evaluation inevitably result in a perception of higher risk for service delivery in an electronic setting?

Liability is most likely to become an impediment to the development of eGovernment if, compared to a paper, telephone or other non-online approach, a particular electronic environment means:

- legal relationships are more complex;
- the visibility and predictability risks is more complicated;
- there is more difficulty in identifying the wrongdoer;
- tracing malignant third parties that have interfered in the communication or service delivery is harder;
- proving the relation between conduct and damage is more difficult;
- much greater damages result from the effect of malfunction within the eGovernment process, as well as inaccuracies in the content.

4.1 Leadership failures (significant)

Leadership plays an important role in identifying and prioritizing liability as a key issue to be considered in all aspects of the design, implementation and use of eGovernment systems and services. Neglecting the importance of such risk management closely relates to possible leadership failure.

Leadership also plays an important role in how the outcome of a cost/benefit analysis is dealt with. Whether or not it is deemed justifiable to take certain risks, or to reject following through on a project because of increased risks, are important decisions that need to be taken, in which leadership is a very important factor.

4.2 Financial inhibitors (very significant)

A cost/benefit analysis is the first step in the development of eGovernment, and can therefore be a crucial obstacle to progress if it highlights negative potential outcomes. Some of these aspects can be coped with by amending legislation, but most relate in one way or another to security measures, particularly their technical and organizational dimensions. A strong link between liability and the financial inhibitors and lack of trust barrier categories is based on the uncertainty that exists with regard to eGovernment risks, particularly legal ones. In the EU, this uncertainty can, at least to some extent, be attributed to a non-existent broader general legal framework regarding liability in Europe.

Financial burdens also arise because of the failure of an eGovernment project or due to obligations to pay for damages caused by a malfunction of, or within, an eGovernment process. Other barrier categories, such as poor technical design, contribute to financial obstacles and therefore need to be taken into account in cost/benefit analyses.

4.3 Digital divides and choices (not significant)

Concerns about liability risks could lead to resistance by some users to going ahead with making use of, or transfer to, electronic government services. However, liability does not have a big influence on the digital divide issue of certain groups not having access to electronic service delivery. Instead, a decision not to enter the world of electronic service delivery more strongly relates to the issue of trust (see Section 5.4.4.6). On the other hand, if fears about liability risk are too large among certain groups, so many people may choose not to use an eGovernment service that a significant obstacle could be created.

4.4 Poor coordination (significant)

Poor coordination of the interpretation and implementation of European legislation and/or the lack thereof is an important barrier related to liability. Poor coordination viewed from a more organizational perspective can also play a role in liability assessment, as this requires cooperation between experts from different scientific disciplines and might involve several government institutions at different levels.

Poor coordination also indicates why it is not only technical features that influence the complexity of related risk assessments or the possible increase regarding liability risks. For instance, the pan-European character of some eGovernment services might complicate the allocation of legal responsibilities or the assessment of these responsibilities. Cross-border activity leads to difficult questions in identifying applicable law and competent forums, as no unified legal framework regarding liability exists in the EU. Thus, the question as to whether there is substantial fear, uncertainty or anxiety regarding legal liability due to differences in national liability law and the lack of harmonization in this field should also be taken into account.

4.5 Workplace and organizational flexibility (significant)

The fear of liability risks can have a significant affect on workplace and organizational flexibility. In Section 5.4.2, several circumstances are described that could be a reason for a reluctance to change from non-electronic to electronic means of communication and service delivery, as well as resistance to the development of new electronic services. This reluctance to initiate eGovernment can be the result of an outcome of a cost/benefit analysis whose interpretation affects the workplace and organizational processes and structures, particularly in the absence of effective management leadership to address relevant issues.

In relation to actions taken by citizens pursuing complaints and compensation (see Section 5.4.4.3), Chatillon (2002) suggests that public servants who administer eGovernment should be reassured by being protected, at least against faults that are due to common errors of care.

4.6 Lack of trust (very significant)

Lack of trust is often described as one of the key barriers to electronic services.⁸¹ In this respect not only trust in government, but also trust in techniques used by government to perform a certain service is of great importance. Liability is one of the relevant factors in generating trust, on the demand as well as supply side. Legal certainty, together with efficiency and cost reduction, can help to attract involvement from businesses in eGovernment.

⁸¹ See Prins et al (2002); Marsh and Dibben (2003); Kossecki (2004).

With regard to lack of trust, liability is one of many points of interest. Whether or not liability leads to financial inhibitors or a lack of trust strongly depends on the circumstances surrounding the eGovernment initiative. For example, the issue of trust can be circumvented by simply imposing the use of a certain eGovernment service by law. However, from a societal and democratic perspective this is not desirable, as eGovernment is something that must be driven by the wishes of the public, instead of being based on government imposition. On the other hand, if interested parties are not troubled by the absence of eGovernment provisions, then there won't be pressure on government from the demand side to introduce such services. In this respect, a link can be made to the barrier of workplace and organizational inflexibility. Legal certainty regarding liability can help to improve trust and, therefore, lower the barrier towards eGovernment. Although amending legislation can create more certainty in this field, this is not a precondition for each eGovernment initiative.

The close relationship between the financial inhibitor barrier and lack of trust is shown when too high a financial risk leads to a lack of trust in using a service or in the delivery of a service. At an operational level, the risk of non-performance or incorrect performance of services is an important ingredient in determining trust levels. The division of liabilities between supply and demand sides also influences trust. Exclusion of liability on the supply side might give the demand side the perception that the service may not be trustworthy. On the other hand, if a supplier is so confident with regard to its service that it accepts all liability, confidence might be boosted on the demand side.

In motivating citizens to become involved in eGovernment, efficiency arguments seem to be of less relevance than: the absence of liability risks; trust in the functioning of the system; and the system's ease to use⁸². Providing a sound legal framework and limiting government scope for placing liability on the users of eGovernment might increase trust to some extent. However, advice and education to build the required capacities could be of greater importance to citizens. Chatillon (2002) emphasizes that citizens' trust in eGovernment requires their complaints to be dealt with a short period of time and with a sufficient amount of compensation. He notes that proceedings in court might be unsuitable, not only from the viewpoint of cost and time effectiveness but also in terms of expertise in understanding failures that can occur in network computing.

4.7 Poor technical design (significant)

Poor technical design is of significance from the perspective of liability mainly in relation to products and software used to establish a European infrastructure for eGovernment and to supply specific eGovernment services. This is a key factor to be taken into account in cost/benefit analyses regarding the development of eGovernment. Another relevant aspect regarding poor technical design is the possibility that national authorities who do not comply with technical standards imposed by the EU or who are responsible for other kinds of technical incompatibilities could be held liable.

5. What are the barriers remaining in this field?

5.1 Difficulty in predicting risks

One of the main problems regarding a cost/benefit analysis in relation to eGovernment services is the lack of predictability. For example, technological turbulence means cost/benefit analyses should be undertaken regularly to support the system's long-term sustainability. However, new technologies for which no experience yet exists make it difficult to foresee possible failures or success rates. Moreover, the lack of predictability

⁸² Anne-Marie Jorritsma (2006), a former Minister in the Netherlands and currently mayor of a Dutch Local Authority, refers to the expectation that electronic government services are complicated as being one of the main reasons for citizens not using eGovernment services.

may in itself lead to a perception of high risks regarding the development of eGovernment. Uncertainty with regard to the functioning of eGovernment processes and the uncertainty of financial and legal consequences of a malfunction can also lead to a lack of trust, on the demand side as well as on the supply side of eGovernment.

There are a number of scenarios relating to reactions to a perceived high risk of liability for a malfunction within an eGovernment process. For example, this may lead government deciding not to make the change from non-electronic to electronic means of communications or service delivery, or to refrain from developing a new kind of electronic service. In this respect, the fear of liability and its consequential financial burdens can form a strong blockage to eGovernment developments.

Another reaction could be that government decides to use limitation and exclusion of liability to lower the risk. Possibilities for insuring the liability risks could also be taken into consideration. However, the insurer will rely on a similar kind of cost/benefit analysis to that undertaken by government. Thus, if the risks related to a certain electronic service are not yet clear, insurance might not be offered or offered only at an extremely high premium.

To avoid the risk of liability, and the potential associated financial burdens, government could also choose to divert liability to other parties involved in the eGovernment process. In this respect, two problems arise. Businesses that government need to involve in the development of eGovernment will themselves use extended exclusions of liability. It is general practice, especially in automation⁸³ contracts, to exclude indirect damages completely. Secondly, government could decide to revert liability to the users of its eGovernment service, which can lead to barriers on the demand side that impede eGovernment.⁸⁴

5.2 Lack of clarity regarding liability law

Clarity with regard to liability, particularly liability law, can facilitate a cost/benefit analysis and thus contribute to the development of eGovernment. However, as already discussed, lack of clarity arising from failures in harmonizing legal rules leads to uncertainty. Therefore, the development of soft law mechanisms or even European legislation to harmonize liability law is, in general, a necessary step towards further development of eGovernment. In this respect, some issues need special attention:

- Clarify the status of different legal provisions to limit or exclude liability, such as the legal status of disclaimers and general terms and conditions (e.g. penalty clauses and limitation of actions), copyright notices and trade mark notifiers.
- Clarify whether or not the government's special position in society leads to the conclusion that government cannot limit or exclude liability.
- Provide principles to be used as a choice of law in order to overcome national differences in liability law, such as strict and fault-based liability as starting points.

Another issue regarding clarity that needs to be taken into account concerns already harmonized fields of liability law. Even though Directives harmonizing certain liability aspects bring some clarity, the achieved level of harmonization is often ambiguous as there remain differences in interpretation of the provisions of the Directive, as well as differences in national implementation laws. An evaluation of the practical impact of the liability clauses in the Directives concerning product liability (e.g. for eCommerce, eSignatures and unfair contract terms) give an insight into the influence these regulatory

⁸³ For information on automations, see Berkvens, van Esch and van Geest (2002).

⁸⁴ If the government finds it necessary to limit or exclude liability to a high degree, this can be interpreted by end users as the eGovernment service not being trustworthy. This is highly relevant issue as studies show the public's use of eGovernment to be particularly low (e.g. Dutton, di Gennaro and Hargrave 2005).

initiatives have had on the development of eGovernment. This can provide relevant information with regard to the more general issue of the need for greater harmonization of liability law at a European level to support progress in eGovernment.

This indicates that legal framework solutions to issues regarding liability are within arm's reach, through the clarification or amending of legislation or the development of soft law mechanisms that could establish the necessary legal certainty.

Sources

Publications

- Berkvens, J. M. A., van Esch and van Geest (2002) (eds), *Automatiseringscontracten, Modellen voor de Praktijk* (losbladig) (pp. 1-52). Deventer: Kluwer.
- Black, H. C. (2004 [1882]), *Black's Law Dictionary*, St Paul, MN: Thomson/West
- Busch D (1998), 'Indirect Representation and the Lando Principles. An Analysis of Some Problem Areas from the Perspective of English Law', *European Journal of Comparative Law*, 2(3), December.
- Chatillon, G. (2002) , Liability and eGovernment: a concept revisited, http://dcss-droit-internet.univ-paris1.fr/bibliotheque/article.php3?id_article=277
- Dutton, W. H., di Gennaro, C. and Hargrave, A. M. (2005), *The Internet in Britain*, Oxford: Oxford Internet Institute, University of Oxford
http://www.oii.ox.ac.uk/research/oxis/oxis2005_report.pdf
- European Commission (2003a), 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)', COM (2003) 702 final, 21.11.2003. http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0702en01.pdf
- European Commission (2003b), *First Report on the Transposition of the Data Protection Directive (95/46/EC)*, 16/5/2003,
http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm
- European Commission (2006a), *Report from the Commission to the European Parliament and the Council on the Operation of Directive 1999/93/EC on a community framework for electronic signatures*, COM (2006) 120 final, 15/03/2006, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0120:EN:HTML>
- European Commission (2006b), *Third Report on the Application of Council Directive on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC of 25 July 1985, amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999)* COM/2006/0496 final, 14/09/2006 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0496:EN:HTML>
- European Group on Tort Law (2005), *Principles of European Tort Law, Text and Commentary*, SpringerWienNewYork, <http://www.egtl.org/>
- Jorritsma, A. M. (2006), 'Nederlandse Zaken, Wake Up Call voor de Digitale Overheid', *Magazine Bestuursacademie Nederland*, February, p. 5
- Markenstein, L. F. (2005), 'Juridische Hordes op de Route naar een Elektronisch Patientendossier (EPD) in de Zorg: Een Inventarisatie van de Stand van Zaken', *Tijdschrift voor Gezondheidsrecht*, 29(5), pp. 368-382.
- Marsh, S. and Dibben, M. R. (2003), *The Role of Trust in Information Science and Technology*, *Annual Review of Information Science and Technology*, 37, pp. 465–98;

- Michel-Verkerke, M. B. and Spil, T. A. M. (2002), Electronic Patient Record in the Netherlands, Luctor et Emergo: But who is Struggling and What Will Emerge?, Enschede, Netherlands: University of Twente, <http://csrc.lse.ac.uk/asp/aspecis/20020088.pdf>
- NECCC (2000), Risk Assessment Guidebook for e-Commerce and e-Government, December 2000, http://www.ec3.org/Downloads/2000/Risk_Assessment_Guidebook.pdf
- Prins, J. E. J., Ribbers, P. M. A., van Tilburg, H. C. A., Veth, A. F. L. and Wees, J. G. L. van der (2002) (eds), Trust in Electronic Commerce: The Role of Trust from a Legal, an Organizational and a Technical Point of View, The Hague: Kluwer Law International.
- von Bar, C. and Drobnič, U. (2003), Study on Property Law and Non-contractual Liability Law as they Relate to Contract Law, http://ec.europa.eu/comm/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/study.pdf
- von Bar, C, Lando, O. and Swann, S. (2002), Communication on European Contract Law: Joint Response of the Commission on European Contract Law and the Study Group on a European Civil Code, European Review of Private Law 2: 183

International and European-level Legislation, Regulations, Conventions and Treaties

- Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Official Journal of the European Communities L 141, 04/06/1999, pp. 20-21, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31999L0034&model=guichett
- Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities L 13, 19/01/2000, pp. 12-20, http://europa.eu.int/information_society/eeurope/i2010/docs/single_info_space/com_el_electronic_signatures_report_en.pdf
- Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities L 178, 17/07/2000, pp. 0001-0015, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML>
- Directive 2002/58/EC of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Communities L 201, 31/07/2002, pp. 37-47, http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf
- Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Official Journal of the European Communities L 210, 07/08/1985, pp. 29-33, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31999L0034&model=guichett
- Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Official Journal of the European Communities L 095, 21/04/1993, pp. 29-34, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:EN:HTML>
- Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, L 281, 23/11/1995, pp. 0031-0050,

<http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

Directive 96/9/EC of 11 March 1996 on the legal protection of databases, Official Journal of the European Communities L 077, 27/03/1996, pp. 20-28,
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31996L0009&model=guichett

Paper 5: Privacy and Data Protection in eGovernment

Cristina Dos Santos and Professor Cécile De Terwangne

CRID, University of Namur, Belgium

1. Description of this legal area

Privacy and the protection of personal data are fundamental rights, which ensue from Article 8 of the European Convention on Human Rights: the right to private and family life, home and correspondence. These rights are now included in a wide range of legislation at European⁸⁵ and Member State levels, as well as in Articles 7 and 8 of the European Charter of Fundamental Rights proclaimed in Nice on 7 December 2000⁸⁶.

Data protection is related to the protection of personal data, which means any information relating to an identified or identifiable person ('data subject')⁸⁷. Data protection rules do not, in principle, prohibit the use of personal data but they offer a legal framework to allow data processing – provided specific requirements are met and special rights are granted to data subjects. The major principles encompassed by such rules are: respect of the purposes of data processing announced at the time of data collection; proportionality (balance between the interest of processing data and the data subjects' interests); and transparency.

A document produced by the independent EU Advisory Body the Article 29 Data Protection Working Party⁸⁸ (2003a) on the protection of individuals with regard to the processing of personal data emphasizes that data protection issues are involved in the development of various types of eGovernment projects and therefore needs careful consideration to ensure the success of these initiatives. Important related issues include the institution of a unique entry point to online administrative services, the institution of unique identifiers – such as personal identification numbers (PINs)⁸⁹ – or even the implementation of interconnections between public databases.

2. How is the area of Data Protection and Privacy related to barriers to eGovernment?

Data protection legislation could certainly be a barrier to eGovernment, as rules on the protection of personal data can prevent or constrain some relevant activities, such as the

⁸⁵ All EU legislation about privacy is available at:

http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

⁸⁶ These are incorporated as Part II in the draft Treaty establishing a Constitution for Europe (see European Commission 2004a and http://europa.eu/constitution/index_en.htm). Presently, the charter is not part of the EU Treaty (for more on the status of the Charter see <http://europa.eu/scadplus/leg/en/lvb/l33501.htm> and the Charter's website: http://ec.europa.eu/justice_home/unit/charte/index_en.html).

⁸⁷ See Directive 95/46/CE, Article 2(a) : "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (also called the 'data subject').

⁸⁸ The Working Party was set up under Article 29 of Directive 95/46/EC and its relevant tasks laid down in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC (for more information see http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm).

⁸⁹ Defined here as in the document of the Council of Europe (1991: Part 5.3), where PINs are conceived in terms of "a unique means of identifying an individual in an administrative file", i.e. a series of numbers used to the identification of a person, by using its birth date, its nationality, its gender, etc (as the security social number in a large number of States, for instance).

processing of information about individuals (and in some countries also of information about legal persons⁹⁰) or the transfer of data to other public bodies and other entities.

The implications of such legislation extend to all eGovernment areas as data protection rules affect: access to public documents containing personal data; the sharing of such documents between different entities; and the re-use of such documents. These rules could therefore hinder the development of businesses offering information services or information products incorporating personal data, including for instance the liability of the 'controller'⁹¹ who determines the purposes and means of processing the personal data.

The contributions of delegations from various European Member States to the Article 29 Data Protection Working Party (2003a) document also highlighted the diversity of the questions dealt with by National Data Protection Authorities in relation to the general framework of eGovernment development. This diversity and the solutions developed to address different contexts, which may sometimes be very different or even conflicting, can be significant blockages to the development of a harmonized European legal framework.

Moreover, according to the European Data Protection Supervisor (EDPS 2006a) the existence of a range of too many actors at all levels (international and European, national, regional and even local) without a common "data protection culture" or shared guidelines could be also a factor of bad governance, because the different interpretations and actions given by different actors could "create substantial and disruptive tensions between stakeholders and in the way services operate in different arenas".

At the European level, Regulation (EC) 45/2001 of the European Parliament (2001)⁹² has therefore established the European Data Protection Supervisor (EDPS)⁹³ to monitor the application of this Regulation's provisions in relation to all processing operations carried out by a Community institution or body (except the Court of Justice acting in its judicial capacity). Each community institution (or body) also needs to appoint at least one person as Data Protection Officer (DPO), who must respond to, and cooperate with, the EDPS⁹⁴. Many efforts are being made by the EDPS to develop a network with these DPOs, under his supervision, to ensure effective compliance with Regulation (EC) 45/2001⁹⁵.

The EDPS and the DPOs recognize not only that all EU bodies needed to appoint a DPO, but that this appointment does not in itself imply automatic compliance with the regulation (see EDPS 2005a). The EDPS therefore emphasizes that "DPOs must be notified adequately of personal data processing within their institution or body (in order to notify the EDPS, where appropriate, of any processing operations that entail specific risks for the people concerned and which therefore need to be checked by the EDPS beforehand)".

⁹⁰ A 'legal person' refers to a company/enterprise or an association recognized by law, in contrast to a 'natural person', who are individual citizens. See Korff (1998) for an examination of the situation in EU Member States with regard to the applicability of their national data protection laws to legal persons, through a comparison between the four Member States that had already applied their data protection laws to legal persons (Austria, Denmark, Italy and Luxembourg) and in five other Member States which did not apply their law in this way (France, Germany, Ireland, the Netherlands and the United Kingdom).

⁹¹ A controller is the person who decides the purpose and means of processing personal data. More formally defined in Article 2(d) of Directive 95/46/EC: "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".

⁹² This Regulation covers the protection of individuals with regard to the processing of personal data by the Community institutions and bodies as well as the free movement of such data, available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_008/l_00820010112en00010022.pdf.

⁹³ The regulation specifies the main duties of the EDPS as covering "supervision", "consultation" and "cooperation" (see <http://www.edps.europa.eu/EDPSWEB/> for more information about the EDPS).

⁹⁴ See the provisions of Article 1, and 24 and following of Regulation (EC) 45/2001 .

⁹⁵ This is a "main objective for 2006" specified by the European Data Protection Supervisor's (2006a) Annual Report for 2005.

This is a problem concerning the transparency of data processing for EU institutions and bodies, and of public administrations more generally.

There are also difficulties of shared competences and liability when many stakeholders share networked resources. In such circumstances, when data is mishandling or errors are created, for instance by uncertainties related to managerial and operational responsibilities in providing content to eGovernment services, it could be very difficult to assign responsibility to a particular entity because there are no general guidelines about assigning such responsibility.

Despite these potential problems, the protection of personal data could be compatible with the development of eGovernment applications, provided an appropriate balance is maintained between the efficiency of administration and the protection of individuals' data. From this perspective, the solutions adopted at the European level regarding European public documents and the protection of the privacy and personal data in those documents could be of great assistance to eGovernment initiatives⁹⁶.

3. What is the European context for this area, including relevant legislation, policy statements and institutional arrangements relevant to this topic?

The right of protection of personal data ensues from different international legislations.

For example, the European Court and the European Commission of Human Rights⁹⁷ have come to regard data protection as a right falling within the scope of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which provides for a right to respect for private and family life, home and correspondence, subject to certain restrictions⁹⁸. Both bodies "regard the [Convention] as a living document which evolves so as to meet new problems". As the European Convention on Human Rights protects also the right to information (see Article 10: "Freedom of expression"), both fundamental rights have been reconciled by the European case law to give them the same protection level beyond national borders.

OECD⁹⁹ (1980) also provided guidelines on the protection of privacy and transborder flows of personal data which would help "to harmonize national privacy legislation of the Member countries (...) [and] to prevent interruptions in international flows of data". These guidelines have represented above all a "consensus on basic principles"¹⁰⁰ which could be built into

⁹⁶ See Opinion 7/2003 on the re-use of public sector information and the protection of personal data, adopted by the Article 29 Working Party on 12 December 2003, available at:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp83_en.pdf

⁹⁷ The case law of the European Commission of Human Rights and the European Court of Human Rights (both organs introduced by the European Convention of Human Rights) was very helpful to the effective definition of the 'right for privacy', then associated to the 'right of personal data protection'. For more information about the European Court of Human Rights, the case law and the Convention, see also: <http://www.echr.coe.int/ECHR>

⁹⁸ Article 8 states: "Right to respect for private and family life: 1. Everyone has the right to respect for his private and family life, his home and his correspondence.; 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

⁹⁹ The Organisation for Economic Co-operation and Development (OECD) was created in 1960 by a Convention. It groups thirty Member Countries, such as Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden, the US, Belgium, Iceland, the Netherlands, Spain or Switzerland. It also has active relationships with some seventy other countries and economies, NGOs and civil society (for more on the OECD see: <http://www.oecd.org>).

¹⁰⁰ Such as "data quality", the "purpose specification principle", "use limitation", "security safeguards", "openness", etc (see OECD 1980: Parts II and III).

existing national legislation, or serve as a basis for legislation in those countries which do not yet have it”¹⁰¹.

The Council of Europe therefore drew up the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981, also known as ‘The Data Protection Convention’ or ‘Convention 108’¹⁰². This convention remains the unique legal binding tool at the international level, with universal application and open to all countries, even those who are not a member of this Council¹⁰³. Some countries have drawn up national data protection laws according to the principles set out by this convention, such as the Irish Data Protection Act of 13 July 1988¹⁰⁴.

Moreover, the United Nations (1990) has also provided some guidelines for the regulation of computerized personal data files in its Resolution 45/95.

Subsequently, the protection of personal data at the European Union level was enshrined in a larger legal framework, such as Article 6 of the EU Treaty and Article 286 of the EC Treaty¹⁰⁵, which reflects work undertaken by the EU and the Council of Europe over a longer period.

This right has been mainly harmonized at European level by two Directives, implemented by Member States: Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and Directive 97/66/EC on data protection in the telecommunications sector, which has been replaced by Directive 2002/58/EC on privacy and electronic communications and the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (amending Directive 2002/58/EC).

Directive 95/46/EC is based on the principles of Convention 108, but has specified and developed them in many ways. In order to provide a high level of protection and a free flow of personal data in the EU, this Directive laid down a general framework for data protection law in Member States. It also established a number of “protection institutional bodies” to control and monitor the appropriate application of the Directive. These include:

- national supervisory authorities (NSAs)¹⁰⁶ (e.g. the Commission for the Protection of Privacy¹⁰⁷ in Belgium; the CNIL¹⁰⁸ in France; the Danish Data Protection Agency¹⁰⁹; and the ‘Garante’ in Italy¹¹⁰);

¹⁰¹ In 1980, some privacy protection laws were introduced in approximately half of OECD Member countries: Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States had passed legislation; and Belgium, Iceland, the Netherlands, Spain and Switzerland had prepared draft bills (see introduction to OECD 1980).

¹⁰² The full text of the Convention N° 108 is available at:

<http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm>

¹⁰³ 35 Countries of the Council of Europe, including all EU Member States, have now ratified it. See Council of Europe website for further information at

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=5/31/2007&CL=ENG>.

¹⁰⁴ Text available at: <http://www.dataprivacy.ie/viewdoc.asp?DocID=64>.

¹⁰⁵ Adopted in 1997 as part of the Treaty of Amsterdam, Article 286 requires that Community acts on the protection of individuals with regard to the processing of personal data; free movement of such data should also apply to Community institutions and bodies, including the establishment of an independent supervisory authority (<http://europa.eu.int/eur-lex/en/treaties/dat/amsterdam.html>).

¹⁰⁶ For more information about websites and national data protection commissioners, see

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm

¹⁰⁷ http://www.privacycommission.be/la_commission.htm

¹⁰⁸ <http://www.cnil.fr/index.php?id=4>

¹⁰⁹ <http://www.datatilsynet.dk/eng/index.html>

¹¹⁰ <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp>

- Article 29 - Data Protection Working Party, which has been implemented by Article 29 of Directive 95/46/EC¹¹¹; and
- a Committee to assist the European Commission on issues related to data protection¹¹².

There is also Regulation (EC) 45/2001 of the European Parliament, which deals with general principles, such as: fair and lawful processing by Community institutions and bodies of personal data; proportionality and compatible use of such data; special categories of sensitive data; information to be given to the data subject; and the rights of the data subject and their supervision, enforcement and remedies.

The rules referred to in Article 286 of the EC Treaty have been laid down in this Regulation¹¹³, which also established the EDPS as an independent supervisory authority at the European level¹¹⁴. Moreover, the EU Treaty establishing a Constitution for Europe (European Commission 2004a) places great emphasis on the protection of fundamental rights, including the protection of personal data. The EDPS (2005) concludes that “this clearly indicates that data protection is now regarded as a basic ingredient of good governance” and emphasizes that “an independent supervision is an essential element of this protection”.

However, despite this European harmonization, there are still important disparities at the Member States level regarding the implementation of Directives related to data protection¹¹⁵. A significant development, as mentioned above, concerns the inclusion or exclusion in the protected data regarding legal persons.

4. What is the relationship of Privacy and Data Protection to the seven barrier categories and associated research questions?

4.1 Leadership Failures (significant)

In his 2005 Annual Report, the EDPS (2006) observed judiciously that the existence of a range of too many actors at different levels without a common “data protection culture” or shared guidelines could be a factor of bad governance, because they could provide different interpretations about the same problems related to data protection and privacy to concerned stakeholders¹¹⁶. Furthermore, there are also problems of different legal frameworks between the EU Member States, together with problems relating to different internal procedures of public bodies and different interpretations given by the national courts to the same issue¹¹⁷. Often, those problems can create a relative legal uncertainty

¹¹¹ The relevant tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC, see also the Article 29 Data protection Working Party website at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

¹¹² Implemented by Article 31 of the 95/46/EU Directive.

¹¹³ Until the adoption of Article 286 of the EC Treaty, there was no legal basis for the Community institutions and bodies equivalent to the legal safeguards of the Directive 95/46/EC, which enabled them to take part in a free flow of personal data and subject with equivalent rules of protection.

¹¹⁴ Its tasks and powers are described in Articles 41, 46 and 47 of the Regulation 45/2001.

¹¹⁵ For further information about such disparities, please consult the website about the status of implementation of Directive 95/46 at

http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm, and all reports about the transposition of the Directive at http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm

¹¹⁶ Similar criticisms were made by participants in the Conference on International Transfers of Personal Data co-organized by the EC, Article 29 Working Party and US Department of Commerce, which has stressed the need for: clearly defined rules for international flows of personal data and for common interpretative opinions relating to international transfers (see more information on http://ec.europa.eu/justice_home/news/information_dossiers/conference_personal_data/index_en.htm).

¹¹⁷ As a member of our expert group, Christopher Kuner (from Hutton&Williams, in Belgium), has outlined: “the lack of uniformity in the definitions of the most basic concepts of data protection law will

about data protection issues, opening up questions like: “how can an adequate level of data protection be guaranteed”¹¹⁸ within this legal “patchwork”?

These problems tend to become more relevant especially when there are cross-border transfers¹¹⁹ of personal data and a lack of central leadership to give formal indications of how to proceed¹²⁰. For some authors, there is a lack of a “unique lock”¹²¹ in the propositions of solutions given by the European authorities regarding data flows with third countries in commercial matters (e.g. the application of the ‘Safe Harbor’ system¹²² in some cases; existence of ‘Binding Corporate Rules’¹²³ within multinational companies; self-regulation).

This issue tends to be highly because many of potential risks related to privacy and data protection are increased when there are so many flows of data in a wider network without frontiers, such as the Internet.

Recently, the European Commission (2007) has adopted a Communication which analyses the past achievements of the ‘Work Programme for better implementation of the Data Protection Directive’¹²⁴, where it noticed that, even if its implementation has improved during last years (all Member States have already transposed it and “on the whole, their transposition covers all the main provisions along the lines of the Directive”), the Commission itself recognizes that this implementation was not “properly” implemented, as some Member States “have failed to incorporate a number of important provisions of the Directive (...) [or] transposition or practice has not been conducted in line with Directive or has fallen outside the margin of manoeuvre left to Member States” (especially regarding the concern of the effective “complete independence” of the national supervisory authorities and the question if they are effectively “endowed with sufficient powers and resources to exercise their tasks”, as it was foreseen by Directive 95/46). For the future “roadmap”, the Commission intends to pursue a policy relying on the future ratification of the Constitutional Treaty (which “would have an enormous impact on this field” by creating “a specific and self-standing legal basis for the Union to legislate in this matter”, between other provisions), even if the Commission does not intend to amend the Directive 95/46.

This leadership failures’ barrier should therefore be overcome by : on the one hand, pursuing “proper implementation” of its provisions at national (and international) level and, on the other hand, by producing “interpretative communications” on some provisions. National data protection supervisory authorities are also invited by Commission to adapt

make it difficult to use eGovernment services across different Member States, since the processing of certain types of data may be subject to substantially different rules” (e.g. different implementations of Article 8 of the Directive 95/46 made by Member States about sensitive data), which “can be a substantial impediment to the take up of eGovernment services”.

¹¹⁸ As was noticed by speakers in the “Introductory welcome speech” at the Conference mentioned in the previous footnote

(http://ec.europa.eu/justice_home/news/information_dossiers/conference_personal_data/intervention_s_en.htm).

¹¹⁹ Regulated by the Articles 25 and 26 of the Directive 95/46/EC (Chapter IV: Transfer of Personal Data to Third Countries). Article 25 contains the “principles” and Article 26 the “derogations”, see: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

¹²⁰ This problem has been taken into account by the European Commission and the Article 29 Working Party (see information about “third countries” that should guarantee an “adequate level” of protection in Article 29 Working Party (2003b) and at:

http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_en.htm).

¹²¹ Remarks made in a speech by Poulet (2006).

¹²² For more about the Safe Harbors framework see:

http://www.export.gov/safeharbor/sh_overview.html, and the various ‘opinions’ 3/2000 and 4/2000 expressed by Article 29 Working Party about it (see

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp31en.pdf and

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp62_en.pdf).

¹²³ For a good analysis of Binding Corporate Rules (BCR), consult the WP 74 of Article 29 Working Party (2003b) (and see examples at:

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/consultations/binding-rules_en.htm).

¹²⁴ Contained by the Commission First report on its implementation (European Commission 2003).

their “domestic practice to the common line they have decided” at the Article 29 Working Party, which should reduce disparities of interpretations, at least at a pan-European level.

4.2 Financial Inhibitors (significant)

Respect for data protection rules could increase costs to implement eGovernment projects (e.g. there must be more than one collection of personal data because a single collection cannot be used for purposes other than those that were contemplated originally). Sensitive personal data (related for instance to health, ethnical origin, etc.) could lead to high costs for the implementation of systems that guarantee effective security. These security mechanisms include also good identification and authentication systems (see Section 5.2) for public officers who need to access to personal data collections to perform their functions (e.g. cost/benefit analyses on the use of PINs and other identifiers and to monitor and assess the impacts on administrative efficiency and effectiveness of data protection and privacy controls). There are also important costs associated with activities undertaken by data subjects in exercising their rights of access, rectification and erasure of personal information collected about them.

4.3 Digital Divides and Choices (significant)

The growing use of ICT has led some public administrations to have more recourse to those identifiers, such as PINs, which could encroach upon personal privacy, especially when they can be used to interconnect different files relating to the person identified. PINs should therefore be kept secure against unauthorized access or dissemination to third parties.

However, there still are big differences between Member States’ legislation about whether or not to use a unique identifier or multi-standard number¹²⁵ (as in Sweden, Denmark, the Netherlands, or Belgium) or a context-specific PIN in several areas of the public administration (as in Austria, Cyprus, France, Germany, or Ireland). These could become obstacles to a uniform, or at least harmonized, European legal framework regarding data protection issues, especially if different ICT systems are used to implement them because they raise specific privacy risks such as the ‘profiling’ of individuals and other security and confidentiality issues’ (see Article 29 Working Party 2002).

Another important aspect is the language barrier at a pan-European level: indeed, as it was outlined by some experts¹²⁶, the “obligation to provide certain information to persons whose data are being processed must take into account the European linguistic diversity” as the real capacity of European citizens to speak or even understand other languages (specially for citizens of new Member States, who sometimes have geographically belonged to another country and need to seek personal data information, e.g. to health problems relating to genetic data). Moreover, this barrier could become more relevant if costs of translation decrease efficiency and effectiveness of cross-border data flows between eGovernment services (this could be also related to the financial inhibitors’ and lack of trust barriers).

¹²⁵ For a good understanding of the risks of using such identifiers, see Keuleers and Dinant (2004). More information is also provided in the Article 29 Data Protection Working Party (2002) opinion on the use of unique identifiers in telecommunication terminal equipment, particularly the Annex which identifies the risks and summarizes the privacy principles that need to be taken into consideration while using a unique identifier in the constitution of IP addresses, and the Article 29 Data Protection Working Party (2000: p. 42) working document on ‘Privacy on the Internet’ which examines the use of global unique identifiers in cookies.

¹²⁶ Comments from Emilio Aced Fález, from our expert group (see footnotes thereafter).

4.4 Poor Coordination (very significant)

There is also the problem of sharing personal data between public bodies and between different countries. For instance, some Member States have opted for a unique entry point to online administrative services oriented toward 'life-events' (e.g. giving birth or changing job) or business-episodes (e.g. employing staff or acquiring a business license¹²⁷). These need to gather information held by different administrative bodies, which means data protection requirements must be monitored and, above all, respected. Here, more than ever, the principle of transparency (see Section 5.6) must be followed by public bodies in all steps of the processing in order to guarantee respect for all legal conditions of Directive 95/46/CE, specially when sensitive data (regarding health, the religion, etc) are processed and transferred between them (e.g. a social security organism could transfer data relating to handicaps to a public employment service portal).

This barrier is also related to the lack of leadership because the solutions adopted by the Member States are very different, sometimes even internally at different levels (national, regional, local).

4.5 Workplace and Organizational Inflexibility (very significant)

With the development of eGovernment, the traditional administrative 'silo model' has shifted to a 'network model' of governance, with functional units linked by digital networks that enables public administrations to communicate internally and externally quickly and efficiently across institutional, political and geographic boundaries. Although from the viewpoint of technological innovation such a networked governance model may be seen as positive progress in itself, the way this could remove the traditional guarantee against 'Big Brother' must be carefully and fully considered to ensure it does not lead to obstacles to eGovernment. For example, data protection regulations could bar access to stored information from certain stakeholders, and they can also prevent the sharing or communication of such data.

The quantity and sensitive nature of personal data processed by public bodies and the compulsory character of its collection indicate that other values must also be considered as important priorities. However, there is often a lack of awareness among some public bodies of the risks linked to data flows, in contrast to the much more acute perception of those risks by the citizens and others using eGovernment services¹²⁸.

4.6 Lack of Trust (very significant)

The main barrier on the demand side is the lack of trust in eGovernment services, such as poor confidence in their security and privacy safeguards and controls systems. The 'eUSER' European web-based survey¹²⁹ regarding eGovernment services has sought to answer the question: 'What do users really want from online public services?'. This gathered important data from ten European countries on a wide range of topics including: access to technologies; the use of the Internet and other ICT-enabled services; the attitudes of end users towards technology in general and the Internet in particular; and users' interaction with providers of services of public interest in the areas of health, education and public administration. The eUSER project is supporting wider policy and

¹²⁷ As at the Banque-Carrefour des Entreprises ('Crossroads-Bank for Enterprises') in Belgium (see: http://mineco.fgov.be/enterprises/crossroads_bank/home_fr.htm).

¹²⁸ See, for example, the eUSER Population Survey 2005 about "Barriers to eGovernment", available on: <http://www.euser-eu.org/ShowCase.asp?CaseTitleID=838&CaseID=1804>

¹²⁹ See the IST-sponsored eUSER project website (<http://www.euser-eu.org>) and the eUSER Population Survey 2005 (<http://istresults.cordis.europa.eu/index.cfm?section=news&tpl=article&ID=81713>).

research activities in the EU to help better address user needs in the design and delivery of eGovernment services.

Among other things, this survey has identified users' fears about supplying personal information online (expressed by 45%) as an "anticipated barrier to eGovernment before use"¹³⁰. Although there are some important differences between countries, there was no distinction between older and newer Member States. For example, fears about supplying personal information online were much higher than average in the UK, Ireland and Hungary.

These 'anticipated barriers' were generally also much higher than the barriers experienced once eGovernment was used. Once citizens have used eGovernment services, the barriers appeared less – though still important – and were related mainly to perceptions of being left alone without sufficient support to assist in solving problems or questions¹³¹. In fact, fewer users have experienced barriers or difficulties (between 17% and 32%) compared with the number of users who perceived barriers before use (between 25% and 58%).

An interesting point to notice is that most citizens have used simple, well-know methods when needing to identify themselves using eGovernment services, such as a user ID/password or PIN code¹³², which are, in contradiction, considered by experts as "the simplest, cheapest and least secure methods and not always suitable" (for instance for legal or financial transactions). Therefore, user identification still remains a barrier to online communication and to services involving transactions, although there is also evidence indicating that more sophisticated methods, such as digital signatures or smart cards, are often rated as being as easy to use as the more well-known methods when they have been provided.

The eUSER survey also demonstrates that there are important differences between countries. Italy, for instance, leads on the use of user ID/password and PIN codes, compared to Poland which has the lowest use of these. Indeed, two of the four new Member States surveyed (Poland and the Czech Republic) did not show the pattern typical of the eight other countries, in which user ID/password and PIN codes are by far the most common methods. The data seem to indicate that in these two countries at least, some focus and investment has been made on more 'advanced' methods, particularly the use of specialized smart cards. In terms of the most advanced methods, Slovenia and Denmark led on the use of digital signatures and the Czech Republic on the use of specialized smart cards. Lastly, the results of the survey stressed that the very high use of credit cards in Ireland is probably related to the fact that some revenue-raising transaction services (such as motor tax) are now fully available online.

Moreover, this lack of trust in eGovernment services and confidence in their security and privacy safeguards and controls can also hold back stakeholders from using some or all eGovernment services because of a fear of an intrusive 'Big Brother' State or that inappropriate use will be made of 'secondary use' of personal information in computer databases.

Another main fear about the security and amount of data communicated to public bodies through electronic media is that the information might be accessed by unauthorized persons, communicated to unauthorized persons or lost because of a technical problem. The more sensitive the data, the more acute is the fear. Moreover, there may be a lack of information about 'who is responsible for what' within the public body due to the

¹³⁰ See http://www.euser.eu.org/eUSER_PopulationSurveyStatistics.asp?KeyWordID=1&CaseTitleID=838 (Chart 10)

¹³¹ See Chart 11 of the survey referenced in the previous footnote.

¹³² See Authentication and Identification in the survey at <http://istresults.cordis.europa.eu/index.cfm?section=news&tpl=article&ID=81713>).

hierarchical structure of civil law public administrations¹³³ – especially if there are problems of liability arising from faults during data collection or in the communication of information to the ‘wrong’ person.¹³⁴

Other related potential obstacles to eGovernment include worries about the lack of transparency of certain personal data processing mechanisms and concerns regarding which countries are suitable for engagement in cross-border information flows containing personal data, as mentioned before.

Furthermore, some data protection experts¹³⁵ stressed the fact that “a further impediment to user trust is the fact that law enforcement (i.e. the “Third Pillar”) activities are currently exempted from the rules of the data protection Directive 95/46. [So] since eGovernment is likely to include the processing of personal data by the police, law enforcement, and similar entities, the present lack of data protection instrument covering such entities can only adversely affect user trust in eGovernment services”. They outline also the fact that firstly “eGovernment is, essentially, the exploitation of technology to offer better and more efficient services to people (...) thus, approaches to eGovernment that do not take into account from the very beginning that they are addressed to the citizens and must be fully respectful with their rights are, in some way, betraying the core concept that lies behind eGovernment”. This is a clear reference to the relatively new concept of ‘eCitizenship’, which “should translate into the digital world the rights afforded to citizens in the real world”¹³⁶, and where the right to privacy and data protection should become a sort of “eRight” (as those rights normally guaranteed and protected by national constitutions).

Even if it is not mentioned in the next point, this barrier remains one of the most important challenge to public administrations in the future in the field of data protection and privacy, that has not yet been resolved regarding the “citizen side”/end-user viewpoint about eGovernment services.

4.7 Poor Technical Design (very significant)

Data protection legislation can introduce a problem of access to stored data: by implementing eGovernment, Member States tend to organize the functioning of their public administrations so as to avoid repetitive requests for the same data to a citizen or enterprise. This implies the sharing of information among the interested bodies.

The favoured technical solution should be one that leaves responsibility for the data with the public authority that first collected it and allows other authorities to access the data, instead of creating a new commonly shared database gathering all the data collected by different authorities (e.g. the Belgian “Social Security Crossroad Bank”¹³⁷). In that case, effective interoperability could provide the right answer from the data protection point of view.

¹³³ See Section 5.1 on Administration Law for more information about this issue. In fact, stakeholders should take into account that, before designing eGovernments projects, the right of a ‘due process’ should also be guaranteed, as people have to give their personal data to public bodies above all because of a legal obligation to do so, so “secondary uses and exchanges of information must be also predictable and not subject to the arbitrary or discretionary decision of a public employee” (this aspect has been also outlined by a member of our expert group – Emilio Aced Fález - from the Data Protection Agency in Madrid, Spain).

¹³⁴ See Section 5.4 on Liability.

¹³⁵ As a member of our expert group, Christopher Kuner (from Hutton & Williams, in Belgium), has stressed to our team. It was also a relevant problem pointed by participants to the Conference on International Transfers of Personal Data co-organized by the EC, Article 29 Working Party and US Department of Commerce, on October 2006 (above mentioned).

¹³⁶ These are some of the important points raised by a member of our expert group, Emilio Aced Fález (above quoted), which outlines also the necessity to have “a public debate about the benefits, opportunities and risks generated by the use of the technology” from the right of privacy perspective.

¹³⁷ See <http://www.ksz-bcss.fgov.be/En/CBSS.htm>

This type of solution was also chosen by the Belgian Walloon Region¹³⁸ in its 'eGovernment and Readability 2005-2009 Plan', which opted for the principle of a unique collection of the personal data of its citizens. This would enable every administrative service (who is authorized by the law to access that information) to find quickly the necessary data nearby the 'authentic source' (which held the information from the beginning and is responsible for the processing, i.e. the 'data controller'¹³⁹). Such a process often takes place by means of a direct communication from application to application, and each search will keep a track of the moving party to guarantee the transparency of the processing to the personal data subject (and this 'track' will be visible when the person concerned accesses his/her personal file).

5. What are the barriers remaining in this field?

5.1 The effective protection of personal data in a networked administration

As mentioned below in Section 5.5.4.5. on workplace and organizational inflexibility, the traditional structure of public administrations was based on a 'silo model', in which each organizational unit within a vertical hierarchy has well-defined competences, with its own information at its disposal to achieve its duties and with its own way of processing that information. This framework resulted in vertical and closed information systems specific to each hierarchical unit. Within it, the communication of information between public bodies was rare and severely regulated. Sharing information with external organizations (e.g. at a different level of administration, a foreign authority or a private-sector organization) was even more restricted.

This vertical framework could therefore be seen until the late 20th Century as a safeguard for citizens against the power of an omniscient State. Since then, eGovernment developments have shifted the silo model towards a 'network model' of governance that enables public administrations to communicate internally and externally quickly and efficiently. While this has much potential to improve efficiency and service, it can also make worse the traditional 'Big Brother' fear as the previous 'paper-based' and 'hierarchical' model was characterized by slow public administration processes which seemed to offer much more protection of citizens' privacy. In these traditional systems, the physical location of documents holding personal data was unique, typically held within the public body that originally collected it. This is no longer the case in eGovernment because the Internet offers more options regarding the speed and flow patterns of data inside a network using methods that are not always under the control of the public administration¹⁴⁰.

5.1.1 Access protection

¹³⁸ More information available at: <http://easi.wallonie.be>

¹³⁹ In the sense of Article 2(d) of Directive 95/46/EC. The controller is therefore linked by virtue of Article 17 of Directive 95/46/EC and "(...) must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected" (http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf).

¹⁴⁰ For instance, in the US there was an example of identity theft (New York Times 2006) by illegal immigrants, who have used fraudulent Social Security numbers of children or dead persons (New York Times 2006). These stolen identities were used to conduct their daily lives (have a job, get a credit, etc) "under the nose" of different public administrations (the Social Security Administration, Internal Revenue Service and Department of Homeland Security). This was done with the knowledge of various actors (their employers, some public officers, etc). Such a case reveals a lack of cooperation between the different services, as they did not share their information in a manner that could permit the situation to be discovered earlier. Key reasons for this were that, on the one hand, IRS Privacy laws prevent the sharing of information and, on the other hand, that illegal immigrants could too easily access to that information by themselves (with no effective sanctions from public officials).

The regulation of access to data to determine who may access what data (and who holds this data) is a crucial potential obstacle to eGovernment expansion. Such access could be facilitated by implementing the 'purpose principle'¹⁴¹: a public body may have access to data only if that is necessary to complete its duties and legal obligations. Moreover, the public body may access only the data that are adequate, relevant and not excessive in relation to the purpose for which they are accessed¹⁴². And citizens must be informed of any shared access to their data¹⁴³.

This kind of solution should not be seen as the independent outcome of a particular individual body (e.g. as a region or a local administrative agency). Instead, it should be regarded as being subject to national guidelines and/or even something like a European 'code of conduct'¹⁴⁴. Such a framework should seek to guarantee aspects like: equality between users at all organizational levels; transparency of personal data processing; and effective interoperability between administrations¹⁴⁵.

In his 2004 Annual Report, the European Data Protection Supervisor (2005b) commented that even Community institutions and bodies were affected by this problem regarding the relationship between public access to documents and data protection. The European Data Protection Supervisor's (2005a) policy paper addresses questions of how promoting public access to documents while protecting personal data entail a clash between two fundamental rights: the right of public access to public documents, as specified in the European Commission's 'Public Access Regulation' 1049/2001¹⁴⁶, and the right to privacy and data protection, as specified in the Commission's 'Data Protection Regulation' 45/2001¹⁴⁷. In his paper, the EDPS maintains that there should not "be a hierarchical order – and often no tension – between both rights, but as the objective of the first was to foster access to all documents, whereas the second must guarantee the protection of personal data, a tension could arise in some cases". The paper concludes that these rights must be seen as complementing, rather than competing with, each other.

This EDPS policy paper also aimed to give practical guidance to EU institutions and/or bodies in cases where there is a need to establish whether a document that contains personal data should be disclosed to a third person. According to Article 4(1b) of Regulation (EC) 1049/2001, the right to public access could be limited by a number of exceptions as it relates to privacy and data protection. However, it imposes three conditions, all of which have to be fulfilled for an exception to public access to apply:

"Privacy of the data subject must be at stake" (but there must be a qualified interest of a person involved).

"Public access must substantially affect the data subject" (and there must be a degree of factual harm to his or her privacy, because the public – intended as the users or the public

¹⁴¹ As stated in Article. 6(1b) of the Directive 95/46/EC: "Member States shall provide that personal data must be: (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards", see: http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf

¹⁴² Article 6(1c) of Directive 95/46/EC.

¹⁴³ According to articles 10 and 11 of Directive 95/46/EC.

¹⁴⁴ This is also the viewpoint of the European Commission (2007).

¹⁴⁵ The 'principle of the 'authentic source' is an example of a promising solution, for instance as implemented by the Belgian National Number Registry. This contains eleven 'legal' personal data items authorized by a law. These allow all public bodies to verify the 'real' identity of a person without knowing other personal data that are not relevant for the activity of those public bodies. For more information on this, see

<http://www.belgium.be/eportal/application?languageParameter=fr&pageid=contentPage&docId=25355>

¹⁴⁶ http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_145/l_14520010531en00430048.pdf

¹⁴⁷ http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_008/l_00820010112en00010022.pdf

institutions – should not be deprived of their right to access if the privacy of the data subject would be only superficially affected by disclosure.)

“Public access is not allowed by the data protection legislation” (here, the principle of the right to information and the principle of proportionality play a key role).

Finally the EDPS (2005a) recommends in a policy paper: “EU institutions and bodies must conduct a concrete and individual examination of each case (...) because compliance with both rights can be enhanced by proactive work, informing the data subjects properly in advance of how personal data will be dealt with – in full respect for the relevant Regulations”¹⁴⁸. This kind of solution is also related to the transparency of the ‘actions’ of the public administration¹⁴⁹, which is closely related to the poor coordination barrier mentioned in Section 5.5.4.4.

5.1.2 Problems of sharing data

Another issue which is related to the barrier of digital divides and choices (Section 5.5.4.3) concerns the problems of sharing data.

Some Member States have established unique entry points to online administrative services¹⁵⁰, which means data protection requirements should be respected when there is a reorganization of the ‘back office’ administrative systems that do not interface directly with citizens and businesses¹⁵¹, but which are linked to the development of such unique entry points. All information converges to the unique entry point, be it on entry or when being used. Here, more than ever, the principle of transparency in all steps of the processing must be followed by public bodies in order to guarantee the respect of all legal conditions of Directive 95/46/CE.

Public administrations that have been developing new services oriented toward ‘life-events’¹⁵² or business-episodes¹⁵³ need to gather information held by different administrative bodies. For example, a family intending to change locality could, if they so desired, have their aggregated data profile analysed by local public administration bodies. Based on this analysis, they could be informed of educational and health facilities, housing entitlements, job opportunities, etc., specific to their family circumstances. While the response might come from multiple agencies, the family would initiate a single ‘life event’ transaction, and would not have to re-supply to each agency involved with the information already gathered by another public body. The response from public administration

¹⁴⁸ Here, as in the European Data Protection Supervisor’s (2006a) Annual Report for 2005, the EDPS also suggested that persons concerned should be given the ability to opt out from disclosure on compelling and legitimate grounds. See document available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2005/AR_2005_EN.pdf.

¹⁴⁹ See Section 5.6 on public administration transparency.

¹⁵⁰ Such as the Belgian “Banque-Carrefour de la Sécurité sociale” (Crossroads Bank for Social Security, as mentioned in earlier footnotes). This has developed networks linking different public bodies by the implementation of a unique key of identification for all information systems (allowed by the law of the 15 January 1990 “Loi relative à l’institution et à l’organisation d’une Banque Carrefour de la Sécurité Sociale”, see: <http://ksz-bcss.fgov.be/En/CBSS.htm>).

¹⁵¹ In the same way as for the Belgian bank mentioned in the previous footnote, a unique entry point for companies can be provided through registration with a company number, etc (see http://mineco.fgov.be/entreprises/crossroads_bank/home_fr.htm).

¹⁵² The term ‘life events’ refers to the government services needed at specific stages in life. Typical examples of life events include: having a baby; starting/leaving school; changing employment status; being a victim of crime; moving home; becoming disabled; retiring; dealing with bereavement (European Commission (2004b)).

¹⁵³ The term ‘business episodes’ refers to the components of the business life cycle. Typical examples of business episodes include: starting a business; employing staff; acquiring a licence; statutory returns; taxation; closing/selling a business (European Commission 2004b). An example of an eGovernment services based on business episodes at the national level can be found in the Irish Government’s Basis site (<http://www.basis.ie>).

agencies would be based on authorized access to aggregate data on the family, and not on individual responses to agency-specific sub-sets¹⁵⁴.

To set up and offer to citizens and enterprises such services, Member States need to be able to link and combine content from multiple and diverse information resources, as well as making sure that all data sharing is managed in a safe way according to data protection principles (purpose limitation, transparency, etc).

For instance, Lefebvre and Poupaert (2002) recommend the implementation of a unique entry point for the Belgian boroughs, and that public bodies should set up a 'digital track' to guarantee in an efficient way the security and the transparency of such processes (i.e. when a public body benefits from a right to access to the personal data of a natural person, this transfer would establish a digital track about which the person concerned would have knowledge). The same kind of "track" would be created for all data processing using the personal data of citizens, which would be available to the person to emphasize the transparency of such operations. In this way, the 'digitization' of data flows would permit a better 'trail' of the personal data processed. The EDPS (2006c) proposes such a trail for e-monitoring of traffic and for budgetary/financial purposes (including the verification of authorized use/access):

5.1.3 A problem of communicating data: self-administration

In some Member States¹⁵⁵, taxation services have adopted a new policy concerning income tax. In this approach, forms are pre-filled by the tax authority before being sent to the concerned person, who has only to check the registered amounts and sign the form. To realize this, the taxation services have to ask several different services to communicate the necessary data. Here too, data protection rules apply, for example requiring the taxpayer to be informed that data collected by another service is being communicated to the taxation authority. This kind of public service must also respect the relevant conditions of Directive 46/95.

Related to: workplace and organizational inflexibility, digital divides and choices, poor coordination, lack of trust

5.2 Interoperability and data protection rules

According to the IDABC (2004): "Interoperability means the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge". This is typical of the way EC official documents treat interoperability, not only in terms of the use and interlinking of large-scale information systems but also with regard to the technical, organizational and semantic (European Commission 2006a) opportunities they open to access or exchange data, or even of sharing or merging databases (European Commission 2006b). The EDPS (2006b) has underlined that this is regrettable "since different kinds of interoperability require different safeguards and conditions".

Data protection does not create any problems in the examples highlighted by the European Commission (2006a) in the areas of cross-border company registration, interoperability in European eProcurement or in the need to reduce the administrative burden on enterprises in the EU through more effective and efficient interoperability¹⁵⁶. However, concerns about data protection legislation are naturally raised as soon as interoperability is seen as a

¹⁵⁴ Example cited in European Commission (2004b).

¹⁵⁵ For example, France (<http://www.impots.gouv.fr/portal/dgi/home?pagelId=home&sfid=00>) and Norway (<http://www.skatteetaten.no/Templates/Emne.aspx?id=2008&epslanguage=NO>).

¹⁵⁶ Except in Member States where information relating to legal persons is protected under the national data protection legislation the same way as information relating to natural persons.

means of serving the exchange, gathering or sharing of personal data (i.e. to “any information relating to an identified or identifiable natural person”¹⁵⁷).

The Commission is conscious of the data protection issues linked to interoperability. It has emphasized that “Pan-European e-Government services need to ensure uniform levels of personal data protection (...) Full compliance with the existing European and national data protection legislation should be ensured. When available, technologies that are privacy-compliant and privacy-enhancing should be used” (IDABC 2004).

In certain documents, however, the Commission focuses mainly on technical and organizational aspects of the concept of interoperability. This has led the EDPS (2006b) to declare that he does not share the view that “interoperability is a technical rather than a legal or political concept”, adding “indeed, it is obvious that making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for de facto acceding or exchanging these data. One can safely assume that technical means will be used, once they are made available; in other words, it is sometimes the means that justify the end and not the other way around. This can lead to subsequent demands for less stringent legal requirements to facilitate the use of these databases: legal changes quite often confirm practices which are already in place”.

This remark seems to be compatible with the communication from the European Commission (2006a) on interoperability for pan-European eGovernment Services: “Technologies and market products are evolving. While new ways of ensuring interoperability are emerging, the increasing potential to enrich eGovernment services means that interoperability is becoming an issue where previously it was not.”

The Commission has also stated: “Interoperability of databases is a key requirement for the development of new added-value services and for cross-border government information services. Furthermore, the interoperability of databases and the information they contain would allow public administration to implement ‘value added’ client-centric services that cannot be implemented on disaggregated information. These would typically involve the provision of client-specific services that can only be determined when client data from multiple sources is aggregated and evaluated as a whole”.

This indicate indicates the need to be conscious at all times of bearing in mind important data protection and privacy issues when sharing and exchanging information.

5.2.1 Interoperability to facilitate the exchange of information v. data protection rules regarding the communication of data

When the concept of interoperability is used as a platform to facilitate the exchange of information, the question of the lawfulness of that communication of data needs to be addressed. In some such circumstances, data protection rules could restrict the communication of personal data. As the EDPS (2006b) has emphasized, even when eGovernment developments do not lead to the creation of new databases they necessarily introduce a new use of existing databases by providing new possibilities for accessing them databases. The EDPS sees this as one of the main reasons why the concept of interoperability has to be examined very carefully.

5.2.2 Interoperability to allow the pursuit of new objectives v. the purpose limitation principle

Large-scale ICT systems allow the pursuit of new objectives that go beyond the original purpose of the data processing objectives of that system. This automatically requires a new and complete analysis of the impact of the current system on the protection of personal data. In this context, the EDPS (2006b) stresses that the interoperability of systems must be implemented with due respect for data protection principles, in

¹⁵⁷ Article 2(a) of the 95/46/EU Directive (above mentioned).

particularly in relation to the 'purpose limitation principle', which the Commission has explained in the context of interoperability as indicating that measures need to be taken "in which individuals have the right to choose whether their data may be used for purposes other than those for which they originally supplied the data in question" (IDABC 2004)¹⁵⁸.

5.2.3 Interoperability and data protection rules on data quality

Rules relating to data quality do not generally impede exchanges of information, but do require that data are communicated only if they are adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed.

5.2.4 Interoperability and the right to correct data

Data subjects are granted the right to obtain, as appropriate, the rectification, erasure or blocking of data whose processing would not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data. The organization of the information system managing and processing the data must guarantee that a request for rectification of data signalled to an organization is transmitted to all connected organizations that have previously accessed the inaccurate data (e.g. in transborder taxation activities).

5.2.5 Interoperability and the duty to inform data subjects

The increased flows of personal data within and between public administrations and their citizens and businesses, including across national borders, has increased the importance of respecting the duty to provide data subjects with appropriate information regarding data processing activities being undertaken on information about that subject, as well as of changes to those activities. This is related to the need to increase transparency in all data processing involving relationships between administrations and citizens¹⁵⁹.

Related barriers: poor coordination, poor technical design

5.3 The introduction and use of PINs

The growing use of ICT has led public administrations to have more recourse to identifiers such as PIN. These could encroach upon personal privacy, especially when they can be used to interconnect different files relating to the person identified. It is therefore necessary for individual countries, and the EU overall, to carefully evaluate the costs of using PINs (e.g. in terms of data protection and privacy problems) and their benefits (e.g. increased administrative efficiency and lower economic costs).

Even if no specific reference to PINs is made in international human rights instruments, a number of international treaties are of particular relevance to the use of PINs, such as the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. For instance, the European Commission of Human Rights has been confronted with issues relating to the

¹⁵⁸ The European Court of Justice (2003) has emphasised in its judgement of 20 May 2003 in the 'Rechnungshof' case the importance of the cumulative application of Articles 6 and 7 of Directive 95/46/EC (for more details see European Court of Justice 2003 and <http://www.curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79969479C19000465&doc=T&ouvert=T&seance=ARRET&where=>).

¹⁵⁹ See, for example, European Data Protection Supervisor (2006a) and the European Ombudsman (2006). Both said that a lot of work has been done by European bodies to guarantee effective access and the right to rectification to personal data, but that there still exists a lack of transparency when personal data are collected (e.g. in answering questions such as: For what purpose? During how much time?) and an overall lack of awareness by citizens about privacy issues. Both also argue that public bodies have a duty to inform citizens about their rights.

use of PINs by public administrations on two occasions ('Lundvall against Sweden'¹⁶⁰ and 'Kolzer against Sweden'¹⁶¹). As the basic principles laid down in the Data Protection Convention are intimately linked to personal data processing, this means that they can undoubtedly help to control the use made of PINs as the key to personal data files.

Furthermore, as the Council of Europe's (1991) Committee of experts on data protection also found, PINs fall within the definition of 'personal data' (taken up by Article 2(a) of the Data Protection Convention and Article 2(a) of Directive 95/46/EC). This implies that some legal barriers must be considered by public administrations in relation to various Articles of the Convention, such as:

- Article 5(a): The data user should obtain a PIN from an individual, company or organization "fairly and lawfully"¹⁶², according to the defined statutory requirement of lawful authority to enable a PIN to be requested from its holder. In the absence of such a justification "the individual's free and informed consent should be sought before the information may be collected".
- Article 5(b): The same principle applies to "the purpose for which a PIN is initially envisaged", in that it "should not be used in a way or for purposes that were not contemplated originally".
- Article 5(c): A PIN should "not be composed of too much personal data in relation to the purpose for which it is to be used".
- Article 5(d): PINs "should be accurate and reflect changes in the circumstances of the bearer".
- Article 6: PINs "should not be composed in such a way as to reveal the categories of sensitive data"¹⁶³ referred to in this Article.
- Article 7: PINs "should be kept secure against unauthorized access or dissemination to third parties".
- Article 8: The holder of a PIN "should be able to exercise rights of access, rectification and erasure"¹⁶⁴ with regard to the data contained on a coded PIN, as well as to the personal data files to which the PIN relates.

These conditions could become legal obstacles to eGovernment at the all levels, for instance because they imply higher costs for the implementation of PINs. However, if they are respected (and they must be respected, as PINs should be considered personal data

¹⁶⁰ See: ECommissionHR, *Lundvall v. Sweden*, Decision of 11 December 1985 (on the admissibility of the application), case 10473/83, *D.R.*, vol. 45, p. 121: "A system of personal identity numbers interferes as such with neither Article 8 nor any other provision of the Convention. As the protection of personal data is covered by this provision, the use of the system may, however, affect the right to respect for private life. There is an interference with a person's right to respect for private life where his name appears in a register of defaulting tax debtors to which the public has access and in spite of the fact that a tax appeal is pending. Interference here considered necessary, bearing in mind local conditions, for the economic well-being of the country and the protection of the rights and freedoms of others (art. 8, §2)".

¹⁶¹ See the ECommissionHR, *Kolzer v. Sweden*, Decision of 13 October 1986 (inadmissible), case 11762/85: "(...) as regards the applicant's complaints about the use of personal identity numbers, the Commission observes that there is no provision in the Convention which as such expressly or implicitly prohibits the use of such numbers. The question which may arise is whether the manner in which personal identity numbers are used infringes any Articles of the Convention. The Commission has previously held that data protection is an issue which falls within the scope of Article 8 (art. 8) of the Convention and that it is conceivable that the use of PINs as a way of storing data in different registers and the matching of such registers could raise an issue under art. 8 (see No. 10473/83, Dec. 11.12.85, unpublished). (...)".

¹⁶² Article 5 is about the "quality of data" collected, which is also treated by Article 6 of the Directive 95/46/EC.

¹⁶³ "The processing of special categories of data" is the aim of the Article 8,1 of Directive 95/46/EC.

¹⁶⁴ Such right of access is also provided by Article 12(b) of Directive 95/46/EC too.

falling within the application of the Directive 95/46/EC¹⁶⁵), they can also be considered as facilitators especially if they increase trust among users by providing legal minimum safeguards and offer transparency for file interconnections. This would be achieved by maintaining always an appropriate balance between privacy requirements and the potential advantages of PINs for public administrations (e.g. in terms of : administrative efficiency; more uniform and manageable methods for identifying persons other than through their names; cost savings; and rapid accurate identification and monitoring). Nevertheless, this could not guarantee the data protection of the individual concerned.

This is important because, as mentioned before (see Section 5.5.4.3), PINs could raise specific privacy risks such as the 'profiling of individuals' and security and confidentiality issues (see Article 29 Working Party 2002): for instance, a PIN originally created as a number issued for the social security context could quickly become an all-purpose standard number/identifier¹⁶⁶. The relationship between data protection and the introduction and use of PINs are also highlighted by specific references to them in certain national data protection laws, such as¹⁶⁷:

- In France, Section 18 of the Law of 6 January 1978 states that the use of the national index identification number with a view to personal data processing may only be authorized by order of the Conseil d'Etat after an opinion from the CNIL¹⁶⁸ (the French data protection authority). The CNIL has built up an extensive case law on the interpretation of Section 18 and has sought to restrict the interpretation of the meaning of the word 'use'.
- In Denmark, data protection legislation governing private registers requires that PINs may be stored by private bodies only if this is authorized by law or if the individual has consented, and provided it is necessary for the body holding the PIN to possess the information to satisfy legitimate requirements.

Furthermore, even in the absence of a specific reference to the competence of data protection authorities to intervene on occasions when the use of PINs raises data protection problems, some national authorities have shown their willingness to police their use. For instance :

- The Swedish Data Inspection Board has asserted its competence when authorities seek to match files with the aid of PINs because the Swedish Data Act stipulates that it is necessary to have the approval of the Board before matching can take place. In accordance with Section 6§1 of this Act, the Data Inspection Board may prescribe how the PIN should be used or it may prohibit the use of the PIN altogether. The same goes for the use of PINs in customer files, for instance the Board is competent to forbid the registration if the disclosure of the PIN of an individual can be considered as an unreasonable condition.

Furthermore, the laws which usher PINs into society may contain specific safeguards regarding their use, as well as for the individuals or bodies competent to use PINs. This is the experience of countries with legislation governing population registers (e.g. Denmark,

¹⁶⁵ By 'deduction' from the case of the EcomissionHR, 'Kolzer v. Sweden', Decision of 13 October 1986 (inadmissible), case 11762/85 (see footnote above).

¹⁶⁶ As noted in Principle 5 of Recommendation (86)1 of the Council of Europe (European Committee on Legal Co-operation/CDCJ) on the on the protection of personal data used for social security purposes (see http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/steering_committees/cdcj/General/1AboutCDCJ.asp#TopOfPage). For CDCJ recommendations before 2000, see http://www.coe.int/t/e/legal_affairs/legal_co-operation/steering_committees/cdcj/documents/2005/CDCJ%20_2005_%205%20e%20-%20List%20of%20treaties.pdf

¹⁶⁷ Country examples mentioned here are drawn from Council of Europe (1991).

¹⁶⁸ See website of the Commission Nationale de l'informatique et des Libertés (CNIL) at: <http://www.cnil.fr/index.php?id=4>

Norway, the Netherlands, Belgium) or which have introduced specific PINs in specific contexts (e.g. Portugal, Switzerland)

There is also no doubt that PINs, in conjunction with automatic data processing, tend to increase the power of public administrations, for instance as file interconnections enabled via the use of unique identifiers allows administrative bodies to match personal information held in various distinct files in a way that excludes the data subject from the information circuit. Moreover, a PIN may not be confined to public sector uses, but also apply to the private sector.

Such assessments of PINs in terms of 'power' raise questions about individual freedoms and control, since the citizen's anonymity is reduced by the existence of an identification number that may stay with the person for life. This makes it easier for the authorities to trace the whereabouts, movements and other activities of citizens and to compile information from different personal data files without their knowledge, then to take decisions on the basis of this accumulated information.

A 'common lecture' of benefits of this identifier and others mentioned above, and the risks raised by them in terms of data protection issues, should be taken into account by an at least harmonized European legal framework, as Directive 95/46/EC only "delegates" to the Member States the power "to determine the conditions under which a national identification number or any other identifier of general application may be processed"¹⁶⁹.

Related barriers: leadership failures, financial inhibitors, digital divides and choices barriers, poor coordination, lack of trust

Sources

Publications

Article 29 Data Protection Working Party (2000), Working Document 'Privacy on the Internet' – An integrated EU Approach to On-line Data Protection, Adopted on 21 November 2000, DG MARKT 5063/00, WP 37, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf

Article 29 Data Protection Working Party (2002), Opinion 2/2002 on the Use of Unique Identifiers in Telecommunication Terminal Equipments: The Example of IPV6, Adopted on 30 May 2002, 10750/02/EN/final, WP 58, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf

Article 29 Data Protection Working Party (2003a), Working Document on eGovernment, Adopted on 8 May, 10593/02/EN, WP 73, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/e-government_en.pdf

Article 29 Data Protection Working Party (2003b), Working Document on Transfers of Personal Data to Third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Adopted on 3 June, 11639/02/EN, WP 74, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

Article 29 Data Protection Working Party (2003c), Opinion 7/2003 on the Re-use of Public Sector Information and the Protection of Personal Data, Adopted on 12 December 2003, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp83_en.pdf

Council of Europe (1991), The Introduction and Use of Personal Identification Numbers: The Data Protection Issues: Study of the Committee of Experts on Data Protection (CJ-PD), Strasbourg: Council of Europe, http://www.coe.int/t/e/legal_affairs/legal_co-

¹⁶⁹ Article 8,7 of Directive 95/46/EC.

[operation/data_protection/documents/reports_and_studies_of_data_protection_committees/X-Pins_1991.asp](http://www.edps.europa.eu/operation/data_protection/documents/reports_and_studies_of_data_protection_committees/X-Pins_1991.asp)

- EDPS (2005a), Position Paper on the Role of Data Protection Officers in Ensuring Effective Compliance with Regulation (EC) 45/2001, Brussels: European Data Protection Supervisor, <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/21>
- EDPS (2005b), Annual Report 2004, 18 March, Brussels: European Data Protection Supervisor, <http://www.edps.europa.eu/EDPSWEB/Jahia/lang/en/pid/22>
- EDPS (2006a), Annual Report 2005, Brussels: European Data Protection Supervisor, 19 April, <http://www.edps.europa.eu/EDPSWEB/Jahia/lang/en/pid/22>
- EDPS (2006b), Comments on the Communication of the Commission on Interoperability of European Databases, 10 March, Brussels: European Data Protection Supervisor, www.edps.eu.int
- EDPS (2006c), Enregistrement des Communications Téléphoniques – Banque Européenne d'Investissement Avis du 8 Mai 2006 sur la Notification d'un Contrôle Préalable à Propos du Dossier Enregistrement des Communications Téléphoniques dans les Salles de Marchés (Dossier 2006-102), Brussels: European Data Protection Supervisor, 8 May, <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/21>
- European Commission (2003), First Report on the Implementation of the Data Protection Directive 95/46/EC, COM (2003) 265 final, 15.5.2003, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2003&nu_doc=265
- European Commission (2004a), EU Treaty Establishing a Constitution for Europe, Official Journal of the European Union C 310, 16 December 2004, <http://eur-lex.europa.eu/JOhtml.do?uri=OJ:C:2004:310:SOM:EN:HTML>
- European Commission (2004b), Linking up Europe: The Importance of Interoperability for eGovernment Services, Staff Working Paper, Brussels: IDA Publications, January, <http://europa.eu.int/idabc/en/document/2036/5583>
- European Commission (2006a), Communication on the Interoperability for Pan-European eGovernment Services, COM (2006) 45 final, 13 February, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2006/com2006_0045en01.pdf
- European Commission (2006b), Application of the Rules on Protection of Personal Data by the Community Institutions and Bodies, March, http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm
- European Commission (2007), Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM (2007) 87 final, 7.3.2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf
- European Court of Justice (2003), Judgment of the Court of 20 May 2003. Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauer (C-139/01) v Österreichischer Rundfunk, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:DKEY=277583:EN:NOT>
- European Ombudsman (2006), Annual Report 2005, Brussels: The European Ombudsman, http://ombudsman.europa.eu/report05/pdf/en/rap05_en.pdf
- IDABC (2004), Final European Interoperability Framework: European Interoperability Framework for pan-European eGovernment Services, version 1.0, November, Luxembourg: Office for Official Publications of the European Communities, 2004, <http://europa.eu.int/idabc/en/document/3473/5585>.
- Keuleers, E. and Dinant J-M. (2004), Data Protection: Multi-application Smart Cards: the use of global unique identifiers for cross-profiling purposes, <http://www.droit-technologie.org> (by courtesy of Computer Law & Security Report), 26 January
- Korff, D. (1998), Final Report of European Commission Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal data relating to such persons, contractor, Study Contract ETD/97/B5-9500/78, October, http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/legal_en.pdf

Lefebvre, A. and Poupaert, N. (2002), Standardisation d'un Guichet Digital et Échange de Données en XLM: Analyse des Aspects Relatifs à la Protection des Données à Caractère Personnel, Report for the SSTC-Privacy Project, University of Namur, Belgium: CRID, October.

Leland J. (2006), Stolen Lives: Some ID Theft is Not for Profit, but to Get a Job, *New York Times*, 4 September, www.nytimes.com

OECD (1980), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: The Protection of Privacy and Transborder flows of personal data; 23rd September, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Poulet, Y. (2006), The Challenges of Applying Data Protection Regimes to Global Data Transfers in Diverse Economies, Keynote speech at the Conference on International Transfers of Personal Data, Brussels, 23-24 October, http://ec.europa.eu/justice_home/news/information_dossiers/conference_personal_data/doc/poulet_speech.pdf

United Nations (1990), 'Guidelines for the Regulation of Computerized Personal Data Files', Resolution adopted by the General Assembly 45th Session on 14 December, A/RES/45/95, http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm

International and European-level Legislation, Regulations, Conventions and Treaties

Note: All EU legislation mentioned is also available at <http://eur-lex.europa.eu/en/index.htm> with all EU legislation about 'privacy' at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950, Council of Europe, <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf>

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (also known as the 'Data Protection Convention' or 'Convention 108'), drawn up within the Council of Europe and opened for signature by the Member States of the Council of Europe on 28 January 1981 in Strasbourg (ETS No. 108); subject to subsequent protocols, http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Data_protection/

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union L 105, 13/04/2006, pp. 54-64, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Union L 201, 31/07/2002, pp. 37-47, http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union L 281, 23/11/1995, pp. 0031-0050, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> [the updated status of implementation see:

http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm].

Directive 97/66/EC of 15 December 1997 of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal of the European Union, L 024, 30/01/1998, pp. 31-50, http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

European Charter of Fundamental Rights for the European Union, Official Journal of the European Union C 364, 18/12/2000, pp. 0001 – 0022 (see also the Charter's website: http://ec.europa.eu/justice_home/unit/charte/index_en.html)

Recommendation (86)1 of the Council of Europe (European Committee on Legal Cooperation/CDCJ) on the on the protection of personal data used for social security purposes (see http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/steering_committees/cdcj/General/1AboutCDCJ.asp#TopOfPage)

Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal of the European Union L 8/1, 12/01/2001, http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_008/l_00820010112en00010022.pdf

Regulation (EC) 1049/2001, of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, Official Journal of the European Communities L 8/1, 12/1/2001, http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_145/l_14520010531en00430048.pdf

Safe Harbor framework, bridges privacy and data protection approaches in the EU and US, http://www.export.gov/safeharbor/sh_overview.html

Treaty Establishing a Constitution for Europe, Official Journal of the European Union C 310, 16 December 2004, <http://eur-lex.europa.eu/en/treaties/dat/12004V/htm/12004V.html>

Treaty of Amsterdam (amending the Treaty on European Union, the Treaties Establishing the European Communities and Related Acts), Official Journal of the European Union C 340, 10 November 1997, <http://europa.eu.int/eur-lex/en/treaties/dat/amsterdam.html>

Websites

Article 29 Data Protection Working Party on data protection, (http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm)

Commission Nationale de l'Informatique et des Libertés (CNIL), the French Data Protection Authority (<http://www.cnil.fr/index.php?id=4>)

Data Protection Commissioners for EU Member States (website links and information available at: http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm)

European Court of Human Rights (<http://www.echr.coe.int/ECHR>)

European Data Protection Supervisor (www.edps.eu.int)

Irish Government's Basis (Business Access to State Information and Services), (<http://www.basis.ie/>)

Conferences, workshops, etc relevant to eGovernment

Conference on International Transfers of Personal Data co-organized by the EC, Article 29 Data Protection Working Party and US Department of Commerce (http://ec.europa.eu/justice_home/news/information_dossiers/conference_personal_data/index_en.htm)

IST 2006 Event, Strategies for Leadership, Helsinki 21-23 November 2006 (http://europa.eu.int/information_society/istevent/2006/index_en.htm)

Research projects

EGovernment Good Practice Exchange (<http://www.ePractice.eu>)

EgovInterop: The eGovernment Interoperability Observatory
(<http://www.egovinterop.net/SHWebClass.ASP?WCI=ShowDoc&DocID=1213&LangID=1>)

EUser – Public Online Services and User Orientation (<http://www.euser-eu.org/Default.asp?MenuID=8>)

IST Results , What users really want from online public services, CORDIS
(<http://istresults.cordis.europa.eu/index.cfm?section=news&tpl=article&ID=81713>)

Case law relevant to eGovernment legal issues

ECommissionHR, *Lundvall v. Sweden*, Decision of 11 December 1985 (on the admissibility of the application), case 10473/83, *D.R.*, vol. 45, p. 121,
<http://cmiskp.echr.coe.int/tkp197/search.asp?sessionid=9794838&skin=hudoc-en>
(search decision with no. and name)

ECommissionHR, *Kolzer v. Sweden*, Decision of 13 October 1986 (inadmissible), case 11762/85,

European Court of Justice, “Rechnungshof” Case, Judgement of 20 May 2003 (about the importance of the cumulative application of Articles 6 and 7 of Directive 95/46/EC), Joint Affairs C-465-00, C-138/01 and C-139/01, <http://www.curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79969479C19000465&doc=T&ouvert=T&seance=ARRE T&where=>

Paper 6: Public Administration Transparency and eGovernment

Professor Cécile de Terwangne

CRID, University of Namur, Belgium

1. Description of this legal area

Public administration transparency relates to the availability to the public of Public Sector Information (PSI) and the transparency of democratic processes (e.g. the holding of open meetings or open online forums). Freedom of Information (FOI) legislation is an aspect of such transparency that plays a significant role in the development of eGovernment services, especially regarding the obligations of 'active transparency' requirements for information to be made publicly available by public authorities. Most FOI Acts are adopted at national (or even regional) level, which brings severe divergences between EU Member States. Associated problematic issues include differences in the exceptions allowed in FOI regulations, such as allowances for public authorities to refuse access to certain public documents (e.g. in case of conflict with data protection rules or national security confidentiality needs). The way those exceptions should be interpreted still needs to be clarified at European level. The only European harmonization that has taken place to date – justified by the principle of Subsidiarity¹⁷⁰ – deals with environmental public documents and transparency for public procurement.

2. How is the area of Public Administration Transparency related to barriers to eGovernment?

Public administration transparency can be categorized as eServices and eDemocracy. Transparency is an expression of eGovernment, which means that barriers to transparency represent barriers to eGovernment. Such barriers can be found in: the lists of exceptions to transparency foreseen in FOI Acts; the lack of public awareness of the availability of a great deal of information; the difficulties in locating information because of the lack of availability of effective 'meta-data' maps to guide seekers in the right direction; the lack of access to appropriate technological tools; or the lack of individual skills to use electronic media well. Traditional FOI Acts are mainly focused on 'passive transparency', which only marginally promotes the active dissemination of PSI. This characteristic of national FOI legislation is not a barrier as such, but shows the limits of such Acts in providing an incentive to the development of information services through the Internet.

Transparency also means access to national information in order to process it and, possibly, to offer pan-European eGovernment services. In this context, even where transparency exists because access to PSI is granted, some barriers can remain to an overall European transparency and to the offer of pan-European services based on this information (e.g. the problem of different languages or restrictions on re-use of received data).

¹⁷⁰ The principle of subsidiarity is "the principle whereby the Union does not take action (except in the areas which fall within its exclusive competence) unless it is more effective than action taken at national, regional or local level. It is closely bound up with the principles of proportionality and necessity, which require that any action by the Union should not go beyond what is necessary to achieve the objectives of the Treaty" (source: http://europa.eu/scadplus/glossary/subsidiarity_en.htm).

3. What is the European context for this area, including relevant legislation, policy statements and institutional arrangements relevant to this topic?

A particular issue regarding access to PSI in the EU is that there is no harmonized regime at EU level for this¹⁷¹. Each country organizes its FOI Acts according to its own administrative regulation and practice.

All Member States have traditionally maintained some form of administrative secrecy for many centuries (Seipel 1996). After important struggles for increased openness, Member States have increasingly adopted FOI Acts that introduce laws and regulations concerning the right of access to the information held by public bodies. All these Acts also contain some exemptions to the guaranteed right of access¹⁷².

Currently, EU-wide legal regimes related to Freedom of Information are limited to the following categories of information and issues:

- freedom of access to environmental information;
- access to information on public procurement; and
- the re-use of PSI.

In the environment domain, the need for harmonization resulted in the adoption of the international Convention of Aarhus (UN/ECE Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters)¹⁷³ signed by the European Community on 25 June 1998, and two European Directives (Directive 90/313 of 7 June 1990 on the freedom of access to information on the environment and Directive 2003/4 of 28 January 2003 on public access to environmental information, repealing Directive 90/313/EEC). Rules regarding time, conditions, restrictions and charges for requests in this area have been determined, as well as principles regarding which information should be made publicly available ('active publicity'), access to justice and determination of the quality of the environmental information.

The European legislative package includes two Directives of particular relevance to public procurement matters: Directive 2004/17 of 31 March 2004, which coordinated the procurement procedures of entities operating in the water, energy, transport and postal services sectors; and Directive 2004/18/EC of 31 March 2004 on the coordination of procedures for the award of contracts for public works, public supply and public service. Questions about information re-use have been addressed in the Directive 2003/98/EC of 17 November 2003 on the re-use of PSI.

Furthermore, Article 255 of the Treaty establishing the European Community¹⁷⁴ guarantees the right of access to documents held by the European authorities (European Parliament, Council and Commission) as a fundamental right granted to every European citizen and to every person resident in an EU Member State. The same right is stated in the Charter of Fundamental Rights of European Union (Article 42). The EU has also adopted Regulation

¹⁷¹ However, note that most of the regimes are based on the content of Resolution R(81) 19 of the Council of Europe. The access regimes are therefore not completely different to each other. Full details of this Resolution is available at:
[http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/administrative_law_and_justice/texts_%26_documents/Conv_Rec_Res/Recommendation\(81\)19.asp](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/administrative_law_and_justice/texts_%26_documents/Conv_Rec_Res/Recommendation(81)19.asp)

¹⁷² Apart from specific information on each Member State legislation, several surveys on national legislation on access to official documents have been consulted, including: European Commission (2000); Council of Europe (2002); European Commission (2003); Banisar (2004; 2006); Kranenborg and Voermans (2005)..

¹⁷³ More information is available at: <http://www.unece.org/env/pp/>

¹⁷⁴ Article 255,§1, of the EU Treaty states that "any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to European Parliament, Council and Commission documents, subject to the principles and the conditions to be defined in accordance with paragraphs 2 and 3" (available at: <http://eur-lex.europa.eu/en/treaties/index.htm>).

1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. This text details the right of access to documents, lists the permitted exceptions to this right and states very interesting duties of active publicity.

On 9 November 2005, the European Commission has also decided to launch a “European Transparency Initiative”¹⁷⁵, which included a review of Regulation 1049/2001 as part of its policy to create more openness¹⁷⁶ among other things. Thus, actually, it has launched a consultation¹⁷⁷ on the review of this Regulation (European Commission 2007b), on the basis of which the Commission will submit proposals for amending it by October 2007.

4. What is the relationship of Public Administration Transparency to the seven barrier categories and associated research questions?

4.1 Leadership failures (significant)

Problems of access to information held by public authorities, or lack of available information can be linked to leadership failures. Political and management leadership in this field requires an ability not only to manage publication and dissemination of PSI projects but also to motivate and support sustained commitment to transparency within public administrations and the use of information services by citizens, media and businesses.

Failures to undertake initiatives to promote transparency where legislation does not impose an obligation to do so will, of course, lead to insufficient dissemination of PSI. In addition, failure to correctly or completely comply with legal obligations also undermines public administration transparency. Leadership failure can also result in: the setting of inadequate deadlines to render information publicly available or to update information; unsatisfactory selection of PSI to be published; and obstructive policy in terms of determining fees to access information that could be too high.

4.2 Financial inhibitors (significant)

Digital dissemination of information can be carried out at a very much lower cost than paper diffusion. When digital dissemination of PSI takes over from printed publications, public administrations are generally in favour of such a change¹⁷⁸. In these cases, costs raised by digital diffusion are not to be considered as a financial inhibitor on the dissemination of PSI.

On the other hand, eGovernment developments have conducive to the arrival of new information services by which certain information is made publicly available that was previously kept internal. In these cases, new costs must be taken into account: mainly

¹⁷⁵ See ‘Green Paper on European Transparency Initiative’ (ETI) (European Commission 2006), which is intended to build on a series of transparency-related measures already put in place by the Commission (e.g. the “access to documents” legislation; the creation of a register of documents; the launch of databases providing information about consultative bodies and expert groups advising the Commission; the wide consultation of stakeholders process; the Commission’s “Code of Good Administrative Behaviour”; etc). A ‘follow-up’ of it (European Commission 2007a) sets out the next steps the Commission will take.

¹⁷⁶ In a Resolution adopted on 4 April 2006 (P6_A(2006) 052), the European Parliament called on the Commission to come forward with proposals for amending the Regulation (EC) No 1049/2001.

¹⁷⁷ This consultation has opened on 18 April and will close on 15 July 2007. The Green Paper is the starting point for this consultation, which allows “any interested person” to have a say on this issue (more information on: http://ec.europa.eu/transparency/revision/index_en.htm).

¹⁷⁸ See for example the Belgian decision (articles 472 to 478 of the law 24 December 2002) to abandon the paper publication of the Belgian official journal, the *Moniteur Belge*, and to publish it exclusively through a website (www.moniteur.be).

personnel costs associated with the time necessary to prepare and elaborate the new information services and to 'feed' them. These costs can represent a financial inhibitor.

4.3 Digital divides and choices (very significant)

One of the main issues concerning transparency of PSI is the digital divides represented by the way knowledge and skills are distributed among users to enable general access to electronic networks, and for finding the location of information specifically being sought among the mass of available online information. This lack can be addressed through education and training programmes or the provision of better service usability, such as through easy-to-understand 'meta-data' guides to help navigation through the information that is available. Multilingual aids are also valuable in bridging digital divides.

Results from the Stakeholder consultation held by the Commission from October to December 2005 (eGov Stakeholder Consultation 2005) indicate with regard to citizen involvement, participation and democracy that, "there is in general the opinion (64%) that eParticipation and eVoting can help or most likely help close the democratic deficit".

4.4 Poor coordination (significant)

The lack of a harmonized regime at EU level with regard to access to PSI, except for environmental information, has already been highlighted, indicating that the European legal landscape concerning public administration transparency is not uniform. However, some harmonization exists, since the principles laid down in Recommendation R(81)19 of the Council of Europe of 25 November 1981 have been used as a model by many Member States.

Structural barriers add to the difficulty. For instance, the federal structure of some States accentuates the disparity of access policies.

Two areas where differences between Member States or regional levels are specially to be noted are in active transparency obligations and the restrictions to access.

4.5 Workplace and organizational inflexibility (significant)

Most EU Member States still need a change of mentality in their public bodies to achieve administration transparency and spontaneous dissemination of PSI. A lack of tradition of openness still too often leads to unjustified withholding of information. Passing from paper publication to digital dissemination through web sites can also be hampered by inflexibility from untrained or unmotivated civil-servants. Management leadership will be of crucial importance to address these kind of difficulties.

4.6 Lack of trust (significant)

Public administration transparency is considered today as a fundamental condition for public trust in government activities, and notably in eGovernment services. This means that access by citizens and private bodies to government information plays a significant role in building trust. Obstacles to building trust can therefore be introduced if there is a lack of openness by public administrations. In many European Member States, there is a lack of tradition for openness and a need for a change of internal culture of government bodies. Trust is closely linked to security issues like authentication and identification (see Section 5.2), as well as to transparency.

4.7 Poor Technical Design (significant)

Digital dissemination of PSI is not always optimally designed, for example as shown by recurrent problems of access to online published information for disabled people¹⁷⁹. More generally, it is often difficult to find one's way to the right information among the mass of available data. Difficulties of access to online information has been stressed at several occasions in consultations with the general public¹⁸⁰.

Developing and publishing meta-data guides to help users identify and locate searched information could greatly improve the accessibility of information.¹⁸¹

5. What are the barriers remaining in this field?

5.1 Restrictions on persons authorized to access public sector documents

At present, Spain is the only Member State that restricts the benefit of the right of access to its own citizens. All other Member States grant this right to every natural or legal person, whatever his/her nationality.

Certain Member States demand the demonstration of a specific interest to grant someone a right of access to official documents, whereas free access without proving any personal interest is generally the rule in most countries, and in EC Regulation 1049/2001. Italy, for example, restricts¹⁸² the right to ask for documents to applicants who have a personal concrete interest to safeguard in legally relevant situations. The Slovenian FOI Act warrants a right of access to documents only to persons showing a well founded legal interest.

Restrictions for applicants are sometimes foreseen only for certain categories of solicited information. In Latvia and Belgium for instance, restricted information (Latvia) or information revealing an evaluation or value judgment on a natural person (Belgium) may be accessed only by persons who declare the purpose for which they wish to access the information.

Related barriers: digital divides and choices

5.2 Practical difficulties of access

5.2.1 Access to, and publication of, documents in electronic media

Not all Member States foresee fully open access to documents in electronic format. Several countries are modifying their legislation to require access to documents in this new format, while others still have paper-based access regimes. When modifying their access regimes, most Member States review at the same time the obligations of Public Authorities regarding the active mandatory publication of PSI in electronic format.

¹⁷⁹ An EC Communication on eAccessibility defined specifically the technical barriers and difficulties experienced by people with disabilities and others when trying to participate on equal terms in the Information Society (see European Commission 2005).

¹⁸⁰ See European Information Directorate General (2006) on the Your Voice on eGovernment 2010 survey and the EU's eUSER research project (<http://www.euser-eu.org>).

¹⁸¹ For examples of meta data guides published to help the citizen know what information is available and where see the Document registers of the European Parliament, the Council of the European Union and the European Commission at: http://europa.eu/documents/registers/index_en.htm

¹⁸² Chapter V (on access to administrative documents) of Italian Act 241 of 7 August 1990 establishing new norms in the administrative procedure and right of access to administrative documents.

This evolution transforms the PSI landscape, making the public sector increasingly aware of the value of its information and the opportunities opened by using its electronic information resources as a new source for improving cost effectiveness (Burkert 1995). The distinction between raw data and value-added data makes less sense in an electronic context, and in some cases the public sector wants to sell its information directly at profit making prices (see Papapavlou (2000)). The roles of public and private actors may therefore be conflicting.

Related barriers: leadership failures, digital divides and choices, poor coordination

5.2.2 Meta-data guides to help locate information

A key reason for failing to access information that is the lack of information and assistance to enable citizens to be aware of what is available and to be guided to locate the documents and other information they require quickly and efficiently.

For information that is passively available, the key issue is to find the authority who should be addressed to obtain the information. For information that has to be published ('active publicity') a citizen must know obviously need to know where it has been published in order to find it. Much time can be wasted during the search process because of the lack of international (and, often, even national) public information storage and organizational rules, including clear information about the documents that come within the 'active' category and the ones for which a request is needed.

As already mentioned, the legal obligation to publish such meta-data exists in some Member States' legislation and in EC Regulation 1049/2001. Several countries ask their public bodies to make publicly available catalogues or registers of the information they hold.¹⁸³ Some legislation specifies that these public registers must be accessible on the Internet.¹⁸⁴ All references to documents are to be recorded in the registers and should identify the subject matter or a description of the content of the document and its date and source. Such public registers are certainly a valuable aid to locating and accessing documents, offering an answer to the problem of insufficient accessibility to official information. It could be of help in achieving these aims if all Member State legislation included a provision imposing the provision of meta-data guides.

Related barriers: leadership failures, digital divides and choices, poor technical design

5.2.3 Cultural barriers

Cultural barriers can be very significant obstacles in achieving public administration transparency. For instance, language can be an important obstacle even when transparency is legally guaranteed in a Member State, as such legislation does not necessarily imply the delivery of information in the language of the person requesting the information, or even an 'international language' such as English.

Related barriers: digital divides and choices

5.2.4 Access fees

In certain countries, fees perceived as being too high are charged for access, discouraging requests for information. Irish law, for example, was amended in June 2003 to impose higher fees "in order to combat abuse of the access rules" (Kranenborg and Voermans: p.81), which led to charges of €15 for a request, €75 for internal review and €150 for review by the Information Commissioner. Most countries explicitly exclude charging for the costs of searching and retrieving the requested documents, except for Ireland and UK

¹⁸³ See Section 5.6.5.6.

¹⁸⁴ See Section 5.6.5.6.

which do impose such costs. For copying documents, the costs are €0.18 per sheet and €3.60 in Austria.

Related barriers: leadership failures, digital divides and choices

5.2.5 Lack of awareness

In all EU Member States, there is a general lack of awareness of the existence of FOI Acts. Even in Sweden, which has had a right of access to official documents for more than two centuries, people are insufficiently aware of their rights and insufficiently exercise them. The Swedish government is aware that¹⁸⁵ “inadequacies exist in terms of knowledge about the public access to information principle. Many citizens have insufficient knowledge of these rights, making it difficult for those citizens to exercise them”. It therefore launched the ‘Open Sweden campaign’ in 2002 to increase public-sector transparency, to raise the level of public knowledge and awareness of information disclosure policies and to encourage active citizen involvement and debate.

This can be a strong obstacle to achieving effective public administration transparency through eGovernment. Overcoming it is most likely to be achieved through information campaigns and other actions to promote awareness, rather than by legislation.

Related barriers: leadership failures, digital divides and choices

5.3 Structural barriers

As mentioned before, the European legal landscape concerning public administration transparency is not uniform. Structural barriers add to the difficulty of the lack of a harmonized European legal environment in this field. For instance, the federal structure of some States accentuates the disparity of access policies. In Belgium, the legal framework is distributed over a federal and several regional levels. In Austria, legal provisions on access to official documents also exist at different internal levels: federal or provincial. In Germany, sectoral laws offer access to specific types of information and some Länder have constitutional provisions and general access laws, with each level adopting different restrictions.

Two areas where differences between Member States or regional levels are specially to be noted are in active transparency activities and the restrictions to access. Recently adopted or recently modified FOI legislations have had two important characteristics: their provisions on active transparency are more detailed and they require the information to be made available through an electronic public network (the Internet). Such provisions are certainly an incentive to eGovernment, in the sense that they oblige public bodies to develop electronic public information services. They also favour eDemocracy developments. However, there are clear differences between national laws on this point, with certain legislation containing detailed provisions while others are totally silent on the same subject (see point 5.3.3.).

Laws and regulations regarding access to PSI contain rules prohibiting the access to information in certain circumstances. Some of the exemptions are very similar in different Member States, but particular legal, historical or political traditions, or other reasons, result in exemptions differing between Member States,¹⁸⁶ For instance: access can be denied if

¹⁸⁵ Cited by Banisar (2004: p. 82).

¹⁸⁶ For example, the Finnish law protects “personal integrity and other important personal interests in health care, social services, taxation or public supervision” (Act 621/99 on the Openness of Government Activities of 21 May 1999), while such precision is not present in other laws. Greek law, for example, foresees an exception to access when “the document concerns the private or the family life of a third party” (Article 5 of Act 2690/1999 Administrative Procedure Code of 9 March 1999). Danish law states that the right of access to administrative documents shall not apply “to personal data” (Danish Access to Public Administration Files Act 572 of 19 December 1985 in 1991 and in

the request is “abusive” (excessive) or obviously formulated too vaguely (in Belgium); seems obviously unreasonable (in Austria and Ireland); or is vexatious (in UK). In some countries (e.g. Hungary¹⁸⁷, Sweden or the Czech Republic¹⁸⁸) confidentiality requirements relating to information access are highly detailed in Secrecy Acts, while this is not the case in other countries.

With regard to constraints on access, some harmonization exists since the contracting parties to the European Convention of Human Rights must abide by the requirements of Article 10, paragraph 2 of the Convention on when restricting access to public documents. This Article specifies that any such restrictions should be: prescribed by law; necessary in a democratic society; and supported by a legitimate aim described in this Article. These legitimate objectives could include:

- being in the interests of national security, territorial integrity or public safety;
- for the prevention of disorder or crime; for the protection of health or morals;
- for the protection of the reputation or the rights of others; for preventing the disclosure of information received in confidence;
- or for maintaining the authority and impartiality of the judiciary.

Related barriers: poor coordination

5.4 Need for changes of government culture

In many European Member States, there is a lack of tradition for openness. Even where legislation now exists to underpin greater administrative transparency, a change of internal culture of government bodies is still needed to achieve this. This is likely to be achieved more through well planned and supported initiatives that challenge effectively traditional organizational cultures than by legislations. The following are some examples of this:

- A study conducted in 2001 and 2002 in the Czech Republic (Otevrete.cz 2002) pointed to problems with “the overuse of commercial secrets and data protection as justifications for withholding, unjustified denials by agencies that claim that they are not subject to the act or simply ignore the law, and a failure of agencies to provide segregable information”.
- In Latvia, problems of practical implementation of the FOI Act have also been signalled. In 2001, following a survey of 200 ministries, Delna (2001) found that “the Latvian government has not devoted sufficient resources to ensuring compliance by state institutions to the laws governing access to information” A follow-up survey held in 2002 and 2003 identified remaining problems of resources, training and education of public authorities. Local government officials were still largely unaware of their responsibilities, even if central government institutions and courts had gained knowledge of transparency new rules. Only one third of the requests received a response in the available legal time frame (Banisar 2004).
- In Slovakia, the Citizen and Democracy Association assessed in 2002 the correctness of implementation of the Act on Free Access to Information. It found that trivial information was usually provided but more “problematic information”, such as contracts and privatization, was most of the time withheld. Moreover, solicited documents were often arbitrarily refused or given only after an attorney’s intervention.

2000). Italian law protects “the privacy of third parties, persons, groups and enterprises” (Chapter V, on access to administrative documents, of Act no 241 of 7 August 1990 establishes new norms on administrative procedure and the right of access to administrative documents) .

¹⁸⁷ A list of 149 categories of information to be considered as ‘State secret’ is annexed to Act LXV on State Secrets and Official Secrets.

¹⁸⁸ 28 types of information listed as subject of being classified into four levels of classification

- Even in Sweden, as discussed in Section 5.6.5.1.3, there has been inadequate implementation of access to meet information rules. A distinctive feature here is that it was the government itself that identified a problem of insufficient openness in practice when it launched its Open Sweden Campaign in 2002. The Swedish government said it found that “clear signals from the public, journalists and trade unions and professional organizations indicate that inadequacies exist in terms of knowledge about the public access to information principle and with respect to its application. Examples of such inadequacies include delays in connection with the release of official document, improper invocations of secrecy...” (Banisar 2004).

Related barriers: leadership failures, workplace and organizational inflexibility, lack of trust

5.5 Insufficient information made publicly available because of legal restrictions of access to official documents

As discussed earlier, blockages to eGovernment created by varying exemptions to the right of access determined by law or other rules in the Member States and in Regulation EC 1049/2001 concerning European authorities can originate from the definition of the scope of national and EC legislation on access to documents, or from the list of exceptions admitted to the principle of access.

Such restrictions can be significant barriers. They can be classified as follows (see also Papapavlou 2000):

- Exemptions in the interest of State (national security, public order, economic interests, international relations, legislative procedures, etc.). For example, some information delivered to the State only for statistical purposes may not be anonymized at the time of collecting the information, so cannot be delivered under access legislation.¹⁸⁹
- Exemptions in the interest of third parties (Intellectual Property Rights, privacy, commercial secrets, judicial procedures, etc.), such as:
- Information protected by IPR will be delivered to the person requesting a copy of a document only with the authorization of the author.
- As the Berne Convention (Article 2 (4)) gives national legislations the discretion to determine the intellectual property protection to be awarded to official texts of a legislative, administrative or judicial nature, a disparity may arise in accessing copyrighted¹⁹⁰ or public domain¹⁹¹ official documents in different Member States.
- When a document relates to private information about a person, it will often not be delivered to a third party without the authorization of the concerned person¹⁹².
- Exemptions to protect the decision-making process (e.g. preliminary or ‘internal use’ information).
- Exemptions to avoid unreasonable workload in the administration concerned (e.g. information already published, excessive requests, vague requests).

Most laws require a ‘harm test’. This examines whether access may, or shall only be, refused as far as disclosure would harm certain protected interests. Some Member States are stricter than others when applying this test. For instance, in some countries access is denied when disclosure could harm (e.g. Czech Republic), would harm (e.g. Estonia,

¹⁸⁹ For example, see the Danish Access to Public Administration Files (Act 572 of 19 December 1985 revised in 1991 and 2000) and the Spanish Law 30/1992 on Rules for Public Administration of 26 November 1992, modified by law 4/99 of 13 January 1999.

¹⁹⁰ This is the case in UK.

¹⁹¹ This is notably the case in Finland, Belgium and France.

¹⁹² This is notably the case in the Slovak law (Act 211/00 of 17 May 2000 on Free Access to Information) and in Belgian law (Loi du 11 avril 1994 Relative à la Transparence de l’administration).

Hungary, Lithuania, Sweden), is reasonably expected to harm (e.g. Ireland) or would cause a concrete damage to (e.g. Italy) a protected interest.

In addition, some exemptions are mandatory and their occurrence prohibits access without any discussion. For others, the public authority involved must balance the public interest in openness and the interests related to preserving secrecy. This 'balance test' (also called 'public interest test') is often performed differently in different cultures.

Related barriers: workplace and organizational inflexibility, lack of trust

5.6 Insufficient and divergent legal duties of active transparency

Access to public sector information can be split into two categories:

- passive: rules determining the information to which access must be given upon request of a citizen, business or another public authority; and
- active: rules regarding information that public authorities have to make spontaneously publicly available without any need for request.

Most EU Member States having laws on access to official documents include duties of government agencies to publish on their own initiative or make available certain categories of information. Instead of being a constraint, these provisions foster development of eGovernment, especially when they require the accessibility of information on the Internet. Serious divergences among national legislations are worth noting in this regard.

A majority of countries¹⁹³ demand their public bodies to release information on their structure, functions, duties, activities, internal rules, procedures or practices, regulations and the interpretation of those regulations. Certain national laws¹⁹⁴ also provide that each authority has the duty to disclose public interest information in their field of activities.

Recently adopted or recently modified FOI legislations require certain kinds of information to be made actively available through the Internet, for example:

- The Estonian Act contains significant provisions regarding electronic access and disclosure of PSI. Public bodies "have the duty to maintain websites and post an extensive list of information on the Internet including statistics on crime and economics; enabling statutes and structural units of agencies; function descriptions of officials, their addresses, qualifications and salary rates; information relating to health or safety; budgets and draft budgets; information on the state of the environment; and draft acts, regulations and plans including explanatory memorandum".¹⁹⁵
- In Poland, public authorities are required to create a Public Information Bulletin to allow access via computer networks to information about their: policies; legal organization; principles of operation; content of administrative acts and decisions; and public assets.¹⁹⁶

¹⁹³ Such requirements, or parts of them, are present in Belgian, Czech, Estonian, Finnish, French, Irish, Lithuanian, Polish, Portuguese, Slovakian, Slovenian, and UK laws.

¹⁹⁴ Hungarian law, for example. Also, the Dutch Act on public access to government information of 31 October 1991 states: "If disclosure of information on the policy of an administrative authority is in the interest of effective, democratic governance, the authority must on its own initiative disclose the information."

¹⁹⁵ Public Information Act of 15 November 2000, RT I 2000, 92, 597.

¹⁹⁶ Act on Access to Public Information of 6 September 2001.

- Article 5 of Slovakian law contains an extensive list of information that has to be disclosed in a way that enables mass access. By 'mass access', the law means accessibility by means of telecommunications, especially through the Internet.¹⁹⁷
- In Slovenia, public authorities have the duty to release information of a public character on the Internet. This includes: consolidated texts of regulations relating to the activities of the public body and its programmes, strategies, views, opinions, studies and other similar documents; proposals for regulations, programmes and strategies; all publications and tendering documentation in accordance with regulations governing public procurements; information on administrative services; and other information of a public character.¹⁹⁸
- Article 5, §2 of the Greek Constitution stipulates: "All persons are entitled to participate in the Information Society. Facilitation of access to electronically handled information, as well as the production, exchange and diffusion thereof constitutes an obligation of the State, always in observance of the guarantees of Articles 9 [protection of a person's home, private and family life], 9A [protection of personal data] and 19 [secrecy of correspondence]."
- EC Regulation 1049/2001 provides that the European institutions are compelled as far as possible to make their documents directly accessible to the public in electronic form or through a register. In particular, legislative documents, which means documents drawn up or received in the course of procedures for the adoption of Acts which are legally binding, are to be made accessible. Where possible, other documents, notably documents relating to the development of policy or strategy, should also be made directly accessible.¹⁹⁹
- Several countries²⁰⁰ ask their public bodies to make publicly available catalogues or registers of the information they hold. Some legislation²⁰¹ specifies that these public registers must be accessible on the Internet.
- International, European and Member States legal texts relating to access to environmental information provide for a wide electronic disclosure of that kind of information.

Related barriers: leadership failures, poor coordination, workplace and organizational inflexibility, lack of trust,

Sources

Publications

- Banisar, D. (2004), The FREEDOMINFO.ORG Global Survey – Freedom of Information and Access to Government Record Laws Around the World, http://www.freedominfo.org/documents/global_survey2004.pdf
- Banisar, D. (2006), Freedom of Information Around the World 2006: A Global Survey of Access to Government Records Laws, July, http://www.freedominfo.org/documents/global_survey2006.pdf
- Beers, T. A. L. (1996), "National secrecy interests versus public access", Conference of Stockholm on access to Public Information, 27-28 June, p.1, <http://europa.eu.int/ISPO/legal/stockholm/en/beers.html>

¹⁹⁷ Article 4, §2 and 6, §1 of Act 211/00 on Free Access to Information of 17 May 2000.

¹⁹⁸ Article 10 of the Act on the Access to Information of Public Character of 25 February 2003.

¹⁹⁹ Article 12 of EC Regulation 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

²⁰⁰ For example, Estonia, France, Latvia, Lithuania, Slovenia, Spain, Sweden.

²⁰¹ For example, Slovenia, Belgium (Flemish Regional level), EC Regulation 1049/2001

- Bunyan, T. (2002), Secrecy and Openness in the European Union, Freedominfo.org, September, <http://www.freedominfo.org/features/20020930.htm>
- Burkert, H. (1995), Public Sector Information: some implications for a European information infrastructure, KnowRight 1995, 133-38.
- Burkert, H. (2006), 'Access Legislation: Some Observations from an Information Law Perspective', in Sjöberg, C. M. and Wahlgren, P. (ed.), Festschrift til Peter Seipel, pp. 95-116.
- Council of Europe (2002), Replies to the Questionnaire on National Practices in Terms of Access to Official Documents, Strasbourg, November 2002, Document Sem-AC(2002)002 Bill to be found at http://www.coe.int/T/E/Human_rights/cddh
- Council of Europe (2003), Rapport l'Accès aux Documents Publics, Groupe des Spécialistes sur l'Accès aux Informations Officielles (DH-S-AC), 10^{ème} Réunion, Strasbourg, September, <http://www.coe.int>
- Delna (2001), 'A Survey of Access to Information in Latvia', Transparency International, <http://www.delna.lv>
- de Terwangne, C. (2004), 'Accès à l'information et Organisations Internationales : le cas de l'Union Européenne', Ethique Publique, Revue Internationale d'Éthique Sociale et Gouvernementale, 6(4), pp. 9-22
- European Commission (2000), Overview of Member States' National Legislation Concerning Access to Documents, Document SG.B.2/VJ/CD D(2000) of 9 October 2000, http://ec.europa.eu/transparency/access_documents/docs/apercu_en.pdf
- European Commission (2003), Comparative Analysis of Member States' and Candidates Countries' Legislation Concerning Access to Documents, http://ec.europa.eu/transparency/access_documents/docs/compa_en.pdf .
- European Commission (2005), Communication on eAccessibility, COM (2005) 425 final, 13.9.2005 http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0425en01.pdf
- European Commission (2006), Green Paper: European Transparency Initiative, COM (2006) 194 final, 3.5.2006, http://ec.europa.eu/transparency/eti/docs/gp_en.pdf
- European Commission (2007a), Communication from the Commission: Follow-up to the Green Paper 'European Transparency Initiative', {SEC(2007) 360}, COM(2007) 127 final, 21.3.2007, http://ec.europa.eu/civil_society/docs/com_2007_127_final_en.pdf
- European Commission (2007b), Green Paper: Public Access to Documents held by institutions of the European Community, COM (2007) 185 final, 18.4.2007, http://ec.europa.eu/transparency/revision/docs/gp_en.pdf
- EDPS (2006), Annual Report 2005, Brussels: European Data Protection Supervisor, 19 April, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2005/AR_2005_EN.pdf
- European Information Directorate General (2006), Your Voice on eGovernment 2010, Online Public Consultation October – December 2005, V1.0, January, Brussels: European Information Directorate General.
- Feral, P-A. (2001), 'L'Accès du Public aux Documents des Institutions Communautaires: la Consécration d'un Droit Fundamental de l'Union Européenne' Jurisclasseur, July, pp. 5 ff.
- IDABC (2005a), eGovernment Observatory, eGovernment News, 13 July, Germany, Legal aspects, <http://www.europa.eu.int/idabc/en/document/4437/5864>
- IDABC (2005b), Study on Stakeholder Requirements for European eGovernment Services, February, <http://ec.europa.eu/idabc/en/document/3880/556>

- Kranenborg, H. and Voermans, W. (2005), Access to Information in the European Union: A Comparative Analysis of EC and Member State Legislation, Groningen: Europa Law Publishing
- Otevrete.cz. (2002), Free Access to Information in the Czech Republic 2000-2002, <http://www.otevrete.cz/index.php?id=142&akce=clanek>
- Papapavlou D. (2000), 'Public Sector Initiatives in the European Union', UNESCO Infoethics 2000, <http://webworld.unesco.org/infoethics2000/>
- Riley, T. B. (2000), 'The Changing Shape of Information and the Role of Government', UNESCO Infoethics 2000, <http://webworld.unesco.org/infoethics2000/>
- Rambøll Management (2004), User Satisfaction and Usage Survey of eGovernment services, Denmark, December
- Seipel, P. (2000), 'Public Access to public sector-held information and dissemination policy – the Swedish experience', Conference of Stockholm on Access to Public Information, 27-28 June 1996, <http://europa.eu.int/ISPO/legal/stockholm/en/seipel.html>

International and European-level Legislation, Regulations, Conventions and Treaties

Note: All EU legislation mentioned is also available at: <http://eur-lex.europa.eu/en/index.htm>

Charter of Fundamental Rights of the European Union, Official Journal C 364, 18/12/2000, pp. 1-22

Directive 2003/4/EC of 28 January 2003 on public access to environmental information, Official Journal of the European Union, L 041, 14/02/2003, pp. 26-32, http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_041/l_04120030214en00260032.pdf

Directive 2003/98/EC of 17 November 2003 on the Re-use of Public Sector Information, Official Journal of the European Union, L 345, 22/06/2001, pp. 90-6, http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_345/l_34520031231en00900096.pdf

Directive 2004/17/EC of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, Official Journal of the European Union, L 134, 30/4/2001, pp. 1-113, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

Directive 2004/18/EC of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, Official Journal of the European Union, L 134, 30/4/2001, pp. 114-240, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en01140240.pdf

Recommendation R(81)19 of the Committee of Ministers to Member States on the Access to Information Held by Public Authorities, adopted on 25 November 1981 [http://www.coe.int/t/e/human_rights/media/4_documentary_resources/CM/1Rec\(1981\)019_en.asp](http://www.coe.int/t/e/human_rights/media/4_documentary_resources/CM/1Rec(1981)019_en.asp) Recommendation (2002) 2 on Access to Official Documents, adopted by the Committee of Ministers of the Council of Europe on 21 February 2002, <https://wcd.coe.int/ViewDoc.jsp?id=262135&Lang=en>

Regulation (EC) 1049/2001, of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, Official Journal of the European Communities L 8/1, 12/1/2001, http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_145/l_14520010531en00430048.pdf

Treaty of Amsterdam (amending the Treaty on European Union, the Treaties Establishing the European Communities and Related Acts), Official Journal of the European Union C 340, 10 November 1997, <http://europa.eu/scadplus/leg/en/s50000.htm>

UN/ECE Convention of 25 June 1998 on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters, Aarhus (DK) <http://www.unece.org/env/pp/>

Websites

Document registers of the European Parliament, the Council of the European Union and the European Commission (http://europa.eu/documents/registers/index_en.htm)

eGouvernement Observatory, a European Commission project to collect and analyse information concerning the main initiatives and developments in the field of eGovernment, in Europe and beyond, and to disseminate this information through the IDABC website and other media (<http://ec.europa.eu/idabc/egovo>)

European Commission, eDemocracy
http://ec.europa.eu/information_society/activities/egovernment_research/focus/edemocracy/index_en.htm

European Commission, eGovernment Good Practice Exchange <http://ec.europa.eu/egov/>

European Commission, eGovernment Research & Development
http://ec.europa.eu/information_society/activities/egovernment_research/index_en.htm

European Commission, Transparency website
http://ec.europa.eu/transparency/index_en.htm

Freedominfo.org: Online network of Freedom of information advocates
(<http://www.freedominfo.org>)

IDABC, the Interoperable **D**elivery of European eGovernment Services to public **A**dministrations, **B**usinesses and **C**itizens designed to help enable the use of information and communication technologies to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe (<http://europa.eu.int/idabc>).

Statewatch Observatory on the adoption of Regulation 1049/2001 EC (FOI in the EU)
(<http://www.statewatch.org/secret/observatory.htm>)

Transparency International, a Berlin-based, worldwide non-profit, non-partisan organization founded in 1993 to curb corruption in international transactions
(<http://www.transparency.org>)

Paper 7: Relationships between Public Administrations, Citizens and Other ICT Actors

Dr Julián Valero Torrijos

University of Murcia, Spain

1. Description of this legal area

One of the main conditions for the success of any initiative related to eGovernment is the guarantee of effective communication between all the parties concerned. From the perspective of citizens, on the one hand it is necessary to ensure that they are able to gain access to electronic public services since the use of ICT may involve new and unexpected obstacles for their relationships with public authorities. On the other hand if a government adopts a too timid policy to promote eServices, the use of ICT will not be perceived as an advantage by users because many of the possibilities offered by private companies in their regular activities – such as bank transfers, sales of travel tickets and general access to information – are not available in the eGovernment services.

Another important issue that must be taken into account in this area concerns the relationships between public administrations and ICT companies. As many eGovernment activities demand a high investment in technology-related resources, both in terms of hardware/software and specialist personnel, the collaboration of these companies is essential because most public administrations do not have the appropriate means to meet these requirements. Nevertheless, it is important to ensure that the final decisions regarding eGovernment systems and services are taken by the public authorities in order to prioritize the protection of public interests. This is especially relevant when defining technological standards for ePublic Services.

2. How is the area of Relationships between Public Administrations, Citizens and Other ICT Actors related to barriers to eGovernment?

Without a general right to use online services in all their relationships with a public administration, citizens may lose confidence in eGovernment, thereby hindering the demand for, and establishment of, new eGovernment services. For instance, the ICT-enabled services frequently made available to citizens may allow only for a narrow range of applications that have been previously and expressly sanctioned by the administration concerned (e.g. to contact the public administration, to return an application form, get information or receive notification of an administrative decisions). As a result, such citizens may find that the only ICT-accessible public services available to them are not those they considered to be most valuable to their own lives. In some circumstances, it may be impractical (e.g. too costly) to implement multi-channel access to a public service, in which case it may be necessary to impose the use of ICT as the only means of contacting a public administration. But this decision can be adopted only when it does not imply discriminatory consequences and ensures access to the public service is available to everyone who needs it.

As for the relationships with ICT companies, there are several potential risks that may involve some barriers from the legal point of view. For instance, it is critical that decisions about the design and use of ICT are not biased toward a particular firm or technology (e.g. a certain operating system or web browser) since they might be contrary to the rules on free competition guaranteed at a European level and by national regulations on public contracts. Technological neutrality must also be extended to those services provided by Trusted Third Parties when their participation is needed to put eGovernment solutions into

action. Otherwise, citizens will be obliged to use only certain commercial products and/or services when there is no technical reason to justify this limitation.

3. What is the European context for this area, including legislation, policy statements and institutional arrangements relevant to this topic?

The European context in this area is analysed in relation to the perspectives of different key actors.

3.1 The perspective of citizens

Although the use of ICT does not necessarily result in a better and more efficient public administration, technological modernization offers a unique opportunity to achieve an appropriate balance between citizens' rights and the efficiency goals of public administrations, as highlighted in the report for the European Commission's Institute for Prospective Technological Studies (IPTS) on eGovernment in the EU in the next decade (Centeno, van Bavel, and Burgelman 2004). This balance is a central challenge for modern democratic public bodies and needs to be emphasized as many Member States are adopting legal obligations for their authorities and civil servants that aim to achieve both good public administration standards and to recognize a related right for citizens to receive such services. Moreover, in some cases this right is guaranteed at the Constitutional level, as in the Finnish Constitution or the Treaty Establishing a Constitution for Europe – commonly referred to as 'EU Constitution' – which is subject to further ratification processes. Many of the principles imposed by this right may be reached more easily through eGovernment tools, such as the right to have one's affairs handled within a reasonable time, the right for citizens to have access to their files or the right to general access to documents.

Another of the pressing demands reinforced by these new principles and by many relevant eGovernment initiatives is the need to go more deeply into a citizen-focused government approach. As the Cap Gemini Ernst & Young (2004) eEurope eGovernment Report warns, services must be developed where citizens receive value in return for their taxes, rather than the services that mostly interest governments. The follow-up Cap Gemini Ernst & Young (2005) report also stresses this perspective, although it concludes that greater improvements have been made in electronic services addressed to companies than to citizens. However, this user-centred philosophy must be supported by legal and institutional changes, for example those outlined by the European Commission (2005a).

The issue of accessibility to eGovernment services must also be considered as a priority. Legal questions about this should be taken into account with some urgency, although online public services have a long way to go before they are fully accessible and inclusive. However, this objective could be considered as Utopian for economic reasons, as explained the European Commission (2004) Report on Multi-channel Delivery of eGovernment Services. Even if complete usability for all groups cannot be achieved, in many countries a restriction on online access to services because of poor design is illegal while in others it is considered discriminatory (e.g. see EPAN 2005). Multi-channel provision should therefore, be considered as the fairest option in order to guarantee the universal access to public services, including at least one electronic and one traditional avenue.

3.2 The perspective of public administrations and ICT companies

According to Centeno, van Bavel, and Burgelman (2004), eGovernment needs to be not only more user-centric but also more networked. This should take account of the growing number of public, private and social actors and intermediaries at EU, national, regional and local levels who are becoming involved in designing and implementing eGovernment

services, as a consequence of a clear tendency towards political decentralization. This demands a serious effort to strengthen coordination and collaboration. One of the most urgent reasons for this is related to interoperability from both a technical and an organizational perspective. As the European Commission's (2006) Communication on interoperability for pan-European eGovernment services has outlined, national programs in this field have encountered serious legal hurdles when trying to simplify processes to support more efficient interaction²⁰². Moreover, as explained in European Commission (2004), the diversity of national legal and administrative systems may become an additional and very relevant blockage to achieving this target, especially at the European level. Promoting the use of open standards²⁰³ and establishing technical standardization criteria at the European level, perhaps through the planned European Institute of Technology²⁰⁴, may be considered as inevitable measures.

The implementation of eGovernment services demands close cooperation between public administrations and ICT companies because of the technological difficulties of this process. However, this collaboration must respect some important legal exigencies. Two key ones are: regulations imposed by the EU Treaties with a general scope related to requirements for free service provision; and those fixed by European and national regulations on public procurement. An example could be of the context-specific implications of these requirements is that those Member States deciding to offer digital signature services associated with electronic Identification (ID) Cards must guarantee the use of alternative digital certificates provided by other public or private Certificated Service Providers; otherwise, Article 4.2 of the *Directive 1999/93/CE on a Community framework for electronic signatures* would be infringed.

4. What is the relationship of this legal area to the seven barrier categories and associated research questions?

The following summarizes the degree to which each of the seven barrier categories used for this research are to legal aspects of relationships between public administrations, citizens and other ICT actors.

4.1 Leadership failures (very significant)

Leadership is a particularly important element in helping eGovernment projects to focus on addressing key issues, such as interoperability problems and the promotion of required legal adaptations, specially when the leading role is played by national authorities. Such leadership is crucial in meeting the needs of citizens and companies.

In relation to interoperability, national regulations on public procurement usually have no specific provisions on technological neutrality. When there is a clear obligation for public authorities to avoid referring to specific brands²⁰⁵, an indirect interdiction could be concluded in order to make eGovernment services available regardless of the software used. However, such software is frequently designed by public administrations, which means such an imprecise obligation is not suitable in these contexts; therefore, more effective legal measures should be adopted. For instance, establishing a clear obligation for public authorities and their private partners and contractors to use technical standards that make electronic services available regardless of the software used by citizens and companies. This is the aim of the Spanish Bill for electronic access of citizens to Public Administrations, which has recognized "technological neutrality" as one of the main

²⁰² <http://ec.europa.eu/idabc/servlets/Doc?id=24117>

²⁰³ As recommended at a eGovernment Policy Stakeholder Meeting in Brussels, 21 September 2005 (see: <http://ec.europa.eu/idabc/en/document/5304/254>).

²⁰⁴ The European Commission has recently approved a proposal for a regulation of the European Parliament and the Council establishing the European Institute of Technology (see: http://ec.europa.eu/education/policies/educ/eit/index_en.html).

²⁰⁵ This is a provision established in many national rules on public contracts, which must also apply to the development of eGovernment applications by private contractors.

principles in the field of eGovernment in order to assure access to eServices and respect for free market rules²⁰⁶.

In promoting legal adaptations, national authorities should also adopt an active position to avoid certain misunderstandings and inconveniences for juridical security. As an example, a main objective of EU regulations is usually to facilitate service provision across all Member States and, therefore, they try to promote free competition and private enterprise. Even more, they do not usually establish excessively restrictive regulations for different contexts since they have no direct competence at more local levels and there is a great diversity among Member States in this field, as an IDABC (2005b) report shows. For instance, the eCommerce Directive has not been conceived to be applicable to the e-activity carried out by public bodies.

This discussion suggests that the main legal problems for technological intermediaries come from national regulations that are not adapted enough to the singularities of ICT and public authorities. Nevertheless, some Directives have established appropriate measures that could facilitate more flexibility in ePublic Services provision (e.g. digital signatures). These may become an obstacle for intermediaries.

4.2 Financial inhibitors (significant)

The generally high cost of implementing multiple channel systems and making eServices available to different disadvantaged groups are often major financial inhibitors. eGovernment inclusivity objectives are required to address these inequalities, by recognizing the rights of citizens and companies to have a choice in how they make contact with public bodies (e.g. online, face-to-face, post, email, telephone).

From the perspective of public–private partnerships, the inflexibility of public procurement regulations is certainly one of the most relevant inconveniences, particularly because of the singularities and restrictions of traditional software contracts. It is necessary for public authorities to ensure contracts include clauses relating to access to the program’s code in order to assure that, in the future, the public body, or a new private partner will be able to adapt the software to new requirements.

Fair competition regulations may also work as an obstacle to establishing network access in certain places (e.g. rural areas) or through modern technologies (e.g. ‘wi-fi’ wireless networks), as they offer no expectation of earning money for private partners while public authorities have neither the experience nor the funds to promote these initiatives. It is essential, then, to develop new business strategies combining public promotion and private partnership that are not based mainly on economic benefit, or are combined with other more profitable activities.

Finally, another relevant problem appears when several public agencies are interested in pooling resources for a common project. In this kind of situation, it could be helpful to create a new organization (e.g. a consortium) with legal capacity in order to assume its own contractual obligations with a separate budget. This could create a stronger capacity for negotiation with ICT companies to achieve better coordination.

4.3 Digital Divides and Choices (significant)

These barriers are relevant in two main areas. Firstly, eGovernment services designed mainly to solve internal administrative problems rather than being conceived primarily to serve the needs of citizens, business and other stakeholders are more likely have poor usability interfaces and interactions. Secondly, compulsory use of electronic public

²⁰⁶ The text of this initiative is available at: <http://www.060.es/>

services may raise constitutional or legal problems if they impede the right of certain groups or individuals to have access to those services.

A new challenge is raised from the perspective of digital divides and the choices made by users when eGovernment offers a new dimension of citizenship with regard to their relationships with public authorities and the way citizens exercise their rights. There is not always clear legal recognition of a new generation of rights covering activities such as access to public communication networks, public information and ePublic Services, as well as the right to 'good' administration and the right not to have to present documents that are already in the hands of public authorities. Even where such rights exist, those citizens without access to eGovernment services may not be covered as they must use traditional means. This means they will not benefit from the opportunities available from the use of an online initiative, such as accessing certain types of documents (e.g. geographic information with added value).

The acceptance of such rights does not always depend on national authorities. Regional and local levels can frequently oppose them at a local level in order to give priority to other issues, perhaps for financial and organizational reasons. General obligations for all public authorities should therefore be promoted in this field by Member States using their competences, although they must bear in mind the degree of technological advance in each society. National Governments can also promote high impact e-services offering the technical tools required to put into action those new rights, as the Danish Government has done with the DanmarksDebatten project²⁰⁷, where a common platform has been created for all public debates taking place within the public sector whether at local, regional or national level.

In addition to the emergence of new rights created by ICT use, some traditional rights are also finding a new dimension in terms of their effectiveness. This consequence is particularly clear regarding information-related issues and the right not to collect twice the same data. As the Belgian Social Security experience shows²⁰⁸, the modernized version of this right has led eServices to citizens often being conceived of as a tool to remedy the problem of the multiple collection of information.

4.4 Poor coordination (very significant)

Coordination is one of the most essential factors in implementing networked ePublic Services and the more general exchange of information between public administrations and other stakeholders. Poor coordination becomes particularly relevant as a barrier when a public organization is based on a decentralized model that supports networked governance processes because effective coordination then becomes a critical requirement in the provision of high quality public services.

The lack of coordination in moving to networked governance models is therefore one of the main legal problems related to interoperability. Since the EU has no concrete competences in this field, this issue may be addressed at the national level, bearing in mind some technical and administrative guidelines promoted at the European level but previously negotiated with national authorities. Although some Member States have established legal obligations in order to achieve technical compatibility, they may need to implement clearer and stricter obligations where they have a direct competence in this field. Otherwise, they can use alternative methods. For instance, a Member State could offer financial aid to regional and local administrations for eGovernment issues when there is a commitment to this requirement. Another alternative, particularly at the local and regional levels, is to try to promote coordination and collaboration through other indirect means, such as technical

²⁰⁷ <http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=230>

²⁰⁸ More details of this experience and its legal implications can be found at <http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=1908>

support or the development of common software. Creating a coordination structure where all the administrative levels are represented is also a desirable measure.

National authorities must also take leadership in adopting ways of indirect coordination, particularly regarding to the promotion of eGovernment services at the local level. For example, national and regional authorities could provide local governments within their jurisdiction with a set of common tools that allows them to offer, at least, all basic services. As shown by the Spanish project Pista Local²⁰⁹, such initiatives may be developed employing an open architecture so that interaction with citizens or other Administrations is guaranteed, regardless of the management system used by each Administration. The German Deutschland-Online²¹⁰ joint strategy for integrated eGovernment must also be emphasized as a relevant experience in order to promote coordination and cooperation between the federal government, federated states and local authorities: they have agreed to develop a joint business model that will be used to offer eGovernment applications developed by the federal government, state governments and municipalities to other regional and local authorities for their use²¹¹.

4.5 Workplace and organizational inflexibility (significant)

Blockages and constraints around workplace and organizational issues focus on the internal perspective of eGovernment services rather than on the needs of citizens, companies and others who are their final users. Inflexibility in this area can therefore be considered as an additional difficulty in promote the changes and adaptations required to modernize public Administration.

4.6 Lack of trust (very significant)

The absence of a wide recognition of citizens' right to contact public administrations through electronic means may involve a lack of trust in eGovernment services, specially if compared with those eServices offered by private companies. Likewise, it is certainly relevant to assure the implementation of eGovernment services with a strict respect of the legal requirements for the use of ICT means; otherwise, a serious risk to the validity and effectiveness of these services could mean citizens will not trust electronic channels since using them might seriously affect their rights. As an example, the recent French Presidential elections raised a relevant controversy; a petition against electronic voting attracted 66.000 signatures because of the doubts over machine error, human error and the malicious actions of hackers²¹².

On the other hand, promoting eGovernment services cannot generally be achieved by restricting how citizens can contact public authorities, particularly when this relationship may become very difficult or impossible. Such restrictions could seriously affect the confidence of citizens and companies in eServices. Although some nuanced arrangements could be made by some Member States, a general obligation of non-discrimination in most would mean those Governments could not rule out a direct and personal contact with citizens since many social groups have no access to electronic means. In addition, if no

²⁰⁹ The operational scheme used in this project is based on a cooperation agreement between the National Federation of Municipalities and Provinces (FEMP) and the Spanish Ministry for Science and Technology, which has allowed FEMP to provide itself with equipment for the maintenance of the product and to facilitate support to the interested county councils and city councils. For further information about Pista Loca, see:

<http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=1847>

²¹⁰ <http://www.deutschland-online.de/>

²¹¹ <http://ec.europa.eu/idabc/en/document/6509/396>

²¹² Further information about this experience can be found at

<http://ec.europa.eu/idabc/en/document/6943/194>

account is taken of this constraint, citizens may not be able to exercise their rights and fulfil their obligations.

This indicates that EU harmonization is not possible, since the concrete social, economical, cultural and technological circumstances of each nation can lead to different requirements and decisions in different contexts. This means that the policies and regulations that are of most practical influence remain at the national or regional level. The EU may suggest alternative systems when public authorities opt to promote the use of ICT from both an internal administrative perspective and for relationships with citizens and businesses, for example through the use of intermediaries such as civil servants or private and specialized agents.

4.7 Poor technical design (not significant)

Poor technical design in areas like user interfaces, interoperability incompatibilities and technical reliability can lead to significant flaws in the usability of eGovernment services, and therefore in the relationships between public administrations, citizens and other actors, such as ICT companies. Although some legal provisions may be adopted in order to improve the technical design of eGovernment software, they cannot be too precise because of the diversity both of services and applications, except in the case of websites where a clear and accessible design can be established by law. Article 53 of the Italian Digital Administration Code can be considered as an example of this kind of measure, although it is only applicable to national Public Administration websites and no measures are provided when they do not respect the legal conditions.

5. What are the barriers remaining in this field?

5.1 The absence of legal obligations to provide electronic public services

As discussed in Section 5.7.2, the lack of confidence in eGovernment caused by the availability of only a narrow range of predetermined services could be addressed by a general right – legally assured – to use online services in all relations with a public administration. This could be a significant factor in promoting a wide understanding of eGovernment services available to citizens and in legally guaranteeing the opportunity to contact the public administration by electronic means to pose any request for information and obtain an effective and quick answer. Unless such a clear legal obligation, public administrations are likely to use their wide discretionary power to prioritize which relationships with citizens can be undertaken electronically.

As public financial resources are limited, and there is strong pressure to use that money in the most efficient and effective way, the intensity of technological eGovernment modernization may vary according to factors other than legal dimensions, such as political considerations, particularly in the case of local administrations. This can lead to eGovernment being seen as a lower priority than other investments, such as building a new and modern hospital. Moreover, technological modernization of public administrations is a very complex process and may demand relevant changes in the organizational culture and habits of civil servants and authorities, which makes it easier to emphasize political options with a lower level of risk and difficulty.

However, public administrations must adapt their activity to take account of technological innovations relevant to exercising their functions; otherwise, there will be a high risk of inefficiency in the operations for which they are responsible. This potential problem must also be assessed from a democratic perspective, taking into account the degree of satisfaction of the groups targeted by public services. Given that many citizens as well as businesses are increasingly getting accustomed to using ICT tools in all other activities of their life in an information society, at least national, regional and medium/large local

Administrations should adopt ICT-enabled solutions not only for their internal administrative activities but also to give a better service to their customers. If they do not assume this obligation spontaneously, a last resort after investigating other options could be to introduce legal obligations to achieve eGovernment aims, such as the EU's eGovernment objectives (see Part 1). This could offer a degree of juridical security, as this kind of measure can enable citizens and companies to know exactly what they should expect from eGovernment services and therefore will be able to demand such provisions.

Despite the relevance of this barrier for eGovernment progression, it cannot be considered as a very severe one since the reluctance of public administrations to offer new and more useful electronic services may be solved through legal changes that can be adopted by the administration concerned, for example by setting clear obligations in a way that overcomes their lack of interest. Public reports ranking the level of electronic public services supply are a useful technique for reaching this goal, although its methodological limitations must be taken into account, specially when they have a European scope. For example, the conclusions of such reports cannot be exhaustive since they cannot bear in mind adequately all the actual contexts of eGovernment services at regional and, above all, local levels.

Therefore, the establishment of legal obligations to provide useful electronic public services must be considered as the most effective way to solve this barrier, although the particular circumstances of each country and the complexity of the services should be taken into account as essential conditions of this decision. A relevant example is the European initiative to promote the compulsory use of electronic means in the field of public procurement through Directives 2004/17/EC and 2004/18 on public procurement. The positive results of this obligation has rapidly appeared, for instance with some Member States, such as France, having already adapted their own legal framework and gone even further than what has been recommended by the European Directives, as explained in the country examples of the eProcurement section of our project's website²¹³.

Related barriers: leadership failures, digital divide and choices, lack of trust

5.2 Interoperability problems

As previously explained, one of the main challenges for public bodies in this field is to achieve a more networked eGovernment service since, in many cases, administrative decisions can be adopted only using information that is the responsibility of other administrative units. If a higher level of efficacy is expected when using ICT, then it will be necessary to automate this kind of communication; otherwise, it won't be possible to make the most of many of the advantages offered by technology, such as the speed in processing large amounts of information; accuracy in searching for data; and efficiency and reliability in updating files. This requirement has been highlighted by the eEurope Action Plan²¹⁴, where it is recognized as a precondition for European eGovernment services and a key issue in providing better services for citizens and companies and ensuring more effective implementation of EU policies. To achieve this, interoperability – especially at a national level – is an elementary requirement in building build European electronic services (e.g. see IDABC 2005).

As the European Commission's (2006) Communication on interoperability for pan-European eGovernment services noted, some Member States have encountered legal hurdles when trying to satisfy this requirement, which becomes a serious obstacle not only for developing national eGovernment programs but pan-European ones as well. This technological problem faces an additional difficulty from the political point of view: many Member States are territorially decentralized and, therefore, fragmentation. This may become a relevant obstacle when local and regional Administrations develop their own

²¹³ <http://www.egovbarriers.org/?view=example&example=procurement>

²¹⁴ See the Plan's website: http://europa.eu.int/information_society/europe/2005/index_en.htm

eGovernment systems. Moreover, as a last resort, this inconvenience may even have significant consequences at the supranational level since European eGovernment services are usually based on the information provided by national, regional and local authorities.

Another potential legal blockage inconvenience to be overcome concerns the way public administrations usually commission private companies to design the information systems and software required to supply their eGovernment services. This kind of collaboration may reveal a new problem in seeking to implement effective interoperability if public interests are not properly guaranteed. For the correct development of eGovernment solutions, it is therefore essential to adopt some legal measures that allow a high level of technical interoperability based on elementary standardization requirements, both for public and private actors.

Even more, from this perspective, it must be emphasized that there are substantive general implications of the increasing deployment of such public-private partnerships (PPIs) in many economic and social fields (see Centeno, van Bavel, and Burgelman 2004). One clear example of how a legal framework can facilitate PPIs is a Finnish initiative²¹⁵ to use bank and Social Security e-IDs for eGovernment services. Here, a regulations were put in place to address interoperability with other identity management systems (including through international interoperability agreements). This has helped to enable the creation of a multi-tiered identification system that encompasses interoperability with other identity management systems.

At the European level, compulsory legal solutions for these questions are often difficult to adopt. Therefore, other measures must be also considered, such as those already put into action through the European Commission's (2006) European Interoperability Framework for pan-European eGovernment Services, which warns that impositions on Member States are not fitting and technical recommendations should be seen only as a proposal. At the European level, the analyzed barrier has serious inconveniences to be overcome from a legal and compulsory point of view, as the EU has no direct competences to help achieve this goal.

In contrast, more severe actions can be taken by Member States as national authorities have concrete legal tools at their disposal, especially if all options are put in action together. When possible, compulsory legal provisions should be adopted following the French Ordinance 2005-1546 on electronic interactions between public services users and administrative authorities, and between Administrations²¹⁶; or the Italian Directive on the exchange of data between administrations and the transparency of negotiation activities in relation to the national eGovernment system that, in order to reduce paperwork, has established that administrations will no longer be able to ask for further supporting documentation and will have to access central databases to cross-check information, although a significant effort is also required to citizens to provide documentation in electronic format and to use eServices where possible²¹⁷. However, this kind of measure cannot always be undertaken, particularly when the state organization is decentralized. In these cases, national authorities may promote soft law measures like the adoption of clear technical standards by the specialized committees in charge of this subject. A German initiative²¹⁸ can be considered as a good example: the Federal Ministry of the Interior has recently published version 2.1 of its Standards and Architectures for eGovernment Applications (SAGA), the German e-government interoperability framework. This is periodically revised and actualized by the Advisory Agency for IT in the Federal

²¹⁵ More details about this initiative are available at:

<http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=200>

²¹⁶ The Ordinance was adopted on 8 December 2005 (available at::

<http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0500286R>).

²¹⁷ For more details about this initiative, visit

<http://ec.europa.eu/idabc/en/document/6683/362>

²¹⁸ Further information on this example can be found at

<http://europa.eu.int/idabc/en/document/4713/336>

Administration (KBSt), an inter-ministerial agency aimed at ensuring that the federal administration optimizes its use of ICT.

Even when these conditions cannot be imposed on regional and local public administrations, it is possible to make financial support to their eGovernment programs – and other ways of collaboration – conditional on the observance of these requirements, although a wide agreement between all public bodies concerned is certainly preferable. This has been the case in the Belgian eGovernment's strategy²¹⁹, which seeks to create a single virtual public administration while respecting the specificities and competences of all government bodies and administrative layers. An agreement was signed in March 2001 by the federal, regional and community authorities to lay down the framework of this cooperation and, particularly, the commitment by all layers of government to use the same standards and the identification infrastructure. This cooperative approach has also inspired the initiative AOC²²⁰ in the Spanish Region of Catalonia, a good example of collaboration between all administrative levels, particularly regional and local, which has been internationally recognized as a nominee for the e-Europe Awards in 2003. One of the main objectives of this project is to share software for eGovernment services with local administrations and, indirectly, contribute to better interoperability.

Some other legal measures could be adopted, although their efficacy in removing blockages to eGovernment progress is relative and diverse. On the one hand, national regulations on public procurement could establish a legal obligation to give preference, according to other circumstances, to the use of certain interoperability standards when selecting the companies that are going to design the software and information systems. Moreover, a general obligation of compatibility for all public administrations should be legally adopted in order to force them, when possible, to use standardized software solutions, although this may not always be as effective as desired because of practical circumstances. The Swiss legal obligation²²¹ to harmonize the country's population registers with other registers of persons is such an example, as it contains precise rules on the content and quality of official registers of persons. It also determines how, and to what extent, data can be used in official statistics and how they can be shared by federal, cantonal and local authorities.

Compulsory measures should specially be adopted inside each public Administration, as the kinds of inconveniences mentioned above cannot be considered as real obstacles from the legal perspective. The Belgian example shows clearly that this is an achievable goal. In 2004, the Belgian Council of Ministers approved new directives and recommendations so that any new ICT system deployed by the federal authorities must be based on open standards, in order to facilitate data sharing and electronic communications with other parties²²².

Related barriers: leadership failures, financial inhibitors, poor coordination, poor technical design.

5.3 The absence of a general right citizens and companies to use ICT

Although the supply of electronic public services has considerably increased in recent years, there is still a need for advancing more deeply in this direction in order to put "Administration électronique au service du citoyens" (Chatillon and Marais, 2003). This new model implies a concept of eGovernment provision based on the effective meeting of the needs of citizens as a priority above satisfying the public bodies' requirements.

²¹⁹ Further information on this example can be found at

<http://ec.europa.eu/idabc/en/document/6608/386>

²²⁰ <http://www.cat365.net>

²²¹ More details about this initiative are available at:

<http://ec.europa.eu/idabc/en/document/6238/5922>

²²² <http://ec.europa.eu/idabc/en/document/3146/360>

However, it is significant that the most established electronic public services typically refer to their fulfilment of internal administrative interests, such as income tax, rather than external needs (Cap Gemini Ernst & Young 2003). In addition, a significant administrative preference is often shown for those services addressed to companies rather than citizens (Cap Gemini Ernst & Young, 2005). This imbalance can be explained by the way in which relationships between public administrations and companies are typically characterized by a higher frequency and complexity, as well as a better profitability from a fundraising perspective. The proposed paradigm of emphasizing citizens' needs can help to offer legal assurance not only to satisfy individuals' requirements but, especially, to improve the democratic legitimation of public bodies.

The absence of a general right for citizens and companies to use electronic means to contact public administrations can be considered as a serious risk for undermining their confidence in eGovernment. In many cases, this can lead to a lack of interest in this channel if citizens' interests are not met. Although some of the implications of this problem have already been examined from the perspective of public administrations, specific nuances of this question from the user's point of view need to be highlighted here. A particular challenge is that it is up to public administrations to decide about the supply of electronic services, which tends to result in priority being given to their own technological modernization needs, such as to enable citizens to contact them and obtain information online. Users can oblige public administration to offer this possibility only when it is legally recognized as their right.

Overcoming this barrier is not easy at a European level because the most useful services for companies and, above all, for citizens are the responsibility of national, regional and local authorities. However, basic freedoms guaranteed by the European Union Treaty – and particularly the achievement of a European common market – may be considered as a relevant argument in order to adopt some measures that necessarily involve the use of ePublic Services, specially for those companies that are established in one Member State and wishes to carry out their activities elsewhere in the EU. However, addressing eGovernment inconveniences to citizens effectively usually depend on solutions relating to national or regional public bodies and authorities (e.g. national or regional Parliaments) with the competence to establish a general right to use eGovernment tools.

It is obvious that the scope of any legal and regulatory measures must be appropriate for the concrete circumstances of the entities concerned and the complexity of the relevant activities. At the same time, in the information society some elementary obligations should be adopted in order to promote eGovernment solutions. For instance, public administrations should generally be legally obliged to offer at least two essential eGovernment services: online access to public information and the ability to obtain application forms through electronic means. If possible, these should be the most useful services for users (both citizens and companies) so that the organizational, technical and financial effort required to provide them would not be seen as disproportionate – especially bearing in mind that the relevant public administration is likely to already have a website and use ICT in their everyday activities. The only exceptions to this obligation could be smaller local administrations where financial limitations could be argued.

Two national examples offer a reference in this field. The Finnish Act on Electronic Service and Communication in the Public Sector²²³ obliges those authorities in possession of the requisite technical, financial and other resources to offer the option of sending a message to a designated electronic address, or another designated device, in order to lodge a matter or to have it considered. On the other hand, the Italian Codice Dell'amministrazione Digitale²²⁴ has established: the minimum set of contents and services available on national public administrations websites; the right to communicate by email for the exchange of documents and information; the need to accept online payments from citizens and

²²³ Chapter 2, Sections 5 and 7 (see: <http://ec.europa.eu/idabc/en/document/6071/392>).

²²⁴ Further information on this example can be found at <http://europa.eu.int/idabc/en/document/4820/5707>

businesses; and a citizen's right to demand that public administration bodies use electronic means in their day-to-day relationship with their publics.

Sometimes it is not possible to recognize a general right immediately, due to organizational and financial problems. Then, the broadening of access channels could be considered, at least in a first step. This is the case in the Estonian project²²⁵ to ensure the availability of a web-based service for citizens and government staff, to enable them to access one hundred government databases and registers. A Spanish example at the regional level is the Generalitat en Red²²⁶ project, promoted by the Government of Valencia as legal standards to support a platform for eServices and to put into action over 200 eServices, more than 80 of which employ eSignature.

Related barriers: leadership failures, digital divide and choices, lack of trust.

5.4 Compulsory use of ICT and access to public services

The promotion of electronic public services cannot be focused on compulsory use of ICT by citizens because that kind of measure may infringe the principle of equity in the access of users to public services. As the IPTS report on eGovernment in the EU in the next decade (Centeno, van Bavel, and Burgelman 2004) warns, one of the main legal requirements in this field is "the need to find the balance between a harmonized framework and mandatory legislation". Moreover, this option can only be considered fair – and sometimes constitutional – if there are no unjustified limitations on the exercise of citizens' and companies' rights, or on the fulfilment of their obligations. Because of the existence of digital divides that affect a wide range of groups in Member States, it is essential to guarantee access to public services regardless of the channel chosen by citizens. The use of at least two channels (one electronic, one more traditional) to gain access to public services should be guaranteed as a rule, to avoid discrimination. As the European Commission (2004b) study *Multi-channel delivery of eGovernment services* emphasizes, "if a user is legally entitled to a service, the administration is legally required to deliver the service".

It must be emphasized here that general solutions at a European level cannot be adopted since the practical conditions for the accessibility of ICT-enabled services are different in each Member State, and for each group of users. Different determining factors in different contexts must be taken into account when establishing new legal provisions seeking to avoid discriminatory consequences. Such differences may make it very difficult or impossible for citizens to access some public services, or even force administrations to fail in the fulfilment of their legal obligations. The Spanish Administrative Procedure Act can be considered an adequate way of combining these requirements in a proportionate way, since the compulsory use of ICT is established only for big companies and public administrations. A Ministerial Order²²⁷ can address the needs of other groups of users, if that measure does not involve restrictions or discrimination. The Estonian solution may also show a way of offering citizens a voluntary option to use electronic means but with a general scope for all communications they receive so as to avoid a double burden on the State: citizens are obliged to choose between the two forms –paper or electronic– and, therefore, those registering for the on-line notification service must waive their right to receive any communication by post²²⁸.

Related barriers: digital divide and choices, lack of trust

²²⁵ More details about this project are available at:

<http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=298>

²²⁶ Complete information about this project can be found at

<http://www.epractice.eu/index.php?menu=4&pn=29&page=gpcase&case=310>

²²⁷ 18th Additional Provision (see: <http://www.map.es>).

²²⁸ More information about the 'Notification Calendar' initiative can be found at <http://ec.europa.eu/idabc/en/document/6399/362>

5.5 The absence of legal obligations to make eGovernment services available

Someone trying to use eGovernment services may find problems with their access to that service because of an inappropriate design of software or because the service can be used only under conditions not appropriate for that user. Diverse situations must be analyzed regarding this barrier since the legal solutions that can be adopted vary greatly. For example, disabled citizens could have a problem of access, access could be too difficult for technical reasons or failure to respect the technological neutrality principle means an ePublic Service can be used only with certain software or equipment, which may not be available to particular users. Overcoming these obstacles would be assured if legally clear overall obligations for public administrations were established. But if that is not the case, it is up to each public body to solve such inconveniences in an appropriate way.

Regarding disabled citizens' access to electronic public services, it is important to mention that the European Commission's (2005b) Communication on electronic accessibility warns about a lack of consistency in this field and, therefore, considers that there should be an improvement in the consistency of accessibility requirements in public procurement contracts in the ICT domain, although Directives 2004/17/EC and 2004/18/EC on public procurement already contain clauses referring to the inclusion of persons with disabilities and older people. This Communication also recognizes that there should be a better use of the 'eAccessibility potential' of existing legislation. As such specialist services are usually offered as an option for disabled or elderly citizens rather than as a standard feature, alternative distance channels should be offered in some cases to ensure access to public services is available in a manner appropriate to each citizen's needs.

From a legal point of view, it is clear that 'soft' provisions included in the aforementioned Directives may be fulfilled, as some Member States have done, in order to tighten the accessibility conditions for disabled people, as shown in the EPAN (2005) report on the eAccessibility of public sector services in the EU, where detailed information about the legal situation in nine countries is summarized. The German Government's approach on this is worth highlighting as its Act on Equal Opportunities for Persons with Disabilities²²⁹ has introduced the right to legal action for any association recognized under the Act. Not going so far, the Austrian Act on eGovernment²³⁰ and the Spanish Act on Information Society Services²³¹ establishes a general obligation for public administrations to make available for disabled citizens the information contained in their websites, and authorizes them to impose these conditions on the companies that design them. The last provision is certainly relevant, and public administrations should adopt it in every case when approving technical specifications for public procurement, particularly with reference to international standards such as the W3C WAI Guidelines²³². Otherwise, no obligations will be assumed by the companies in charge of designing websites or developing software for providing eGovernment services.

The design of eGovernment systems can also become an obstacle for the relationships between public administration and private individuals if it hinders the utilization of software or operating systems owned by citizens, especially if they are obliged to purchase a licence for certain commercial products and cannot use other common programs, including free open source software. Thus, it is essential to ensure legally the technological neutrality of the applications used to transmit administrative information and establish online relationships between public administrations and citizens. This should be expressly guaranteed by the rules regulating the contracts between public administrations and the enterprises that create the software.

Related barriers: leadership failures, financial inhibitors, digital divide and choices, lack of trust, poor technical design

²²⁹ Available at: <http://www.cabinetoffice.gov.uk/e-government/resources/eaccessibility/index.asp>

²³⁰ <http://europa.eu.int/idabc/servlets/Doc?id=21448>

²³¹ <http://www.lssi.es>

²³² <http://www.w3.org>

5.6 Restrictions on multi-channel access to eGovernment services

The use of electronic media may offer significant advantages for citizens and companies compared to more conventional channels. However, the new media can also threaten the achievement of inclusivity and equity goals, as it could exclude many who do not have the finance, skills and support to enable them to make effective use of eGovernment capabilities. This could be a real barrier if there is compulsory use of ICT, but otherwise it could be regarded as essentially a perceived legal barrier with social and/or economic implications, since it may not be possible to establish direct legal consequences if the decision about whether to use electronic public services or more conventional ones is regarded as a voluntary choice.

However, there is a clear exception when a public administration decides to use electronic means to speed up its processing of applications through the use of ICT because the information needed has already been processed or can be collected faster. In such cases, it would be desirable to fix some specific legal limits, especially where other citizen's rights may be affected, such as in competitive procedures relating to the awarding of financial subsidies. Although a clearer regulation should be adopted, this kind of problem could also be easily solved without any legal reform. For instance, it could be sufficient to apply current rules in a prudent way. Moreover, in certain cases this kind of problem can be overcome through purely organizational measures, such as enhancing the personal face-to-face service provided at the traditional administrative office in order to make available the same information as offered through the Internet.

Related barriers: financial inhibitors, digital divide and choices, lack of trust, workplace and organizational flexibility

Sources

Publications

- Cap Gemini Ernst & Young (2004), Online Availability of Public Services: How is Europe Progressing? Report of the Fourth Measurement October 2003, Brussels: European Commission, Directorate General for Information Society and Media, http://europa.eu.int/information_society/eeurope/2005/doc/highlights/whats_new/capgemini4.pdf
- Cap Gemini Ernst & Young (2005), Online Availability of Public Services: How is Europe Progressing? Report of the Fifth Measurement October 2004, Brussels: European Commission, Directorate General for Information Society and Media, http://ec.europa.eu/information_society/soccul/egov/egov_benchmarking_2005.pdf
- Centeno, C., van Bavel, R. and Burgelman, J.-C. (2004), eGovernment in the EU in the Next Decade: The Vision and Key Challenges, Technical Report EUR 21376, Brussels: Institute for Prospective Technological Studies (IPTS), European Commission, <http://europa.eu.int/idabc/servlets/Doc?id=19131>
- Chatillon, G. and Marais, B. du (2003), Administration Electronique au Service du Citoyens, Brussels: Bruylant
- EPAN (2005), eAccessibility of Public Sector Services in the European Union, an EPAN (European Public Administration Network) report, London: Cabinet Office (e-Government Unit), available at: [http://www.cabinetoffice.gov.uk/e-government/docs/eu_accessibility/pdf/eaccessibility\(eu\)_report.pdf](http://www.cabinetoffice.gov.uk/e-government/docs/eu_accessibility/pdf/eaccessibility(eu)_report.pdf)
- European Commission (2004b), Multi-channel Delivery of eGovernment Services, Brussels: European Commission, Enterprise DG, <http://ec.europa.eu/idabc/servlets/Doc?id=16867>

European Commission (2005a), CoBrA Recommendations to the eEurope Advisory Group, Brussels: European, Commission, (DG Information Society, eGovernment Unit), <http://ec.europa.eu/idabc/servlets/Doc?id=18465>

European Commission (2005b), Communication on Electronic Accessibility COM (2005) 425 final. http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0425en01.pdf

European Commission (2006): Communication on Interoperability for Pan-European eGovernment Services Interoperability for Pan-European eGovernment Services, COM (2006) 45 final, <http://europa.eu.int/idabc/servlets/Doc?id=24117>

IDABC (2005), eGovernment in the Member States of the European Union, Brussels: European Commission, IDABC eGovernment Observatory, <http://ec.europa.eu/idabc/servlets/Doc?id=21035>

Valero, J. (2004), Régimen Jurídico de la e-Administración, Granada: Comares.

International and European-level Legislation, Regulations, Conventions and Treaties

Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities L 13, 19/01/ 2000, pp. 12-20, <http://europa.eu.int/ISPO/docs/policy/docs/399L0093/en.pdf>

Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities L 178, 17/07/2000, pp. 0001-0015, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML>

Directive 2004/17/EC of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, Official Journal of the European Union, L 134, 30/4/2001, pp. 1-113, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

Directive 2004/18/EC of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, Official Journal of the European Union, L 134, 30/4/2001, pp. 114-240, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en01140240.pdf

Websites relevant to eGovernment legal issues

eGovernment Good Practice Exchange (<http://www.egov-goodpractice.org>).

IDABC, the service for the Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens to help enable the use of information and communication technologies to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe (<http://europa.eu.int/idabc>).

Paper 8: Re-Use of Public Sector Information in eGovernment

Professor Cécile de Terwangne
CRID, University of Namur, Belgium

1. Description of this legal area

Public sector information (PSI) is unique. As Herbert Burkert (1995) explains: “Public sector information is not only the basis of public sector decision making, it also contributes essentially to the informational infrastructure of our societies. Its features are unique. It can – where necessary – be collected under a legal obligation on the information provider. It is associated with neutrality. It provides an ‘informational backbone’ to economic and social activities.” The private sector has a great interest in this data as it may represent a unique source of certain information, while the public sector also has an interest in its own re-use of the data.

Public bodies gather details about citizens, business enterprises, land use, public decisions, vehicles, food, meteorology, health and most other sectors of society. Such public databases spread over different public services are being increasingly computerized, and eventually may all be compatible with each other. This will make exchanges between databases technically possible, even if that may not be desirable or legally valid from some perspectives. Public sector information is therefore of great value, particularly in an electronic environment.

In EU Directive 2003/98/EC on the re-use of public sector information, usually referred to as the ‘PSI Directive’, ‘re-use’ is defined as the use by persons or legal entities of documents held by public sector bodies for commercial or non-commercial purposes other than the initial purpose related to the public task for which the documents were produced. The exchange of documents between public sector bodies purely in pursuit of their public tasks does not constitute such re-use.

According to this Directive, re-use should aim to facilitate “the creation of Community-wide information products and services based on public sector documents, to enhance an effective cross-border use of public sector documents by private companies for added-value information products and services...”²³³. This should be allowed only when carried out with total transparency and in a way that limits distortions of competition in the EC. Everyone should know the conditions under which re-use can occur and whether competition rules are respected.

2. How is the area of the Re-Use of Public Sector Information related to barriers to eGovernment?

Many eGovernment services depend on the re-use of information gathered or produced by public administrations, whether that re-use is proposed by the public sector itself or by interested private actors. For example, a national taxation department may offer a new service to persons interested in knowing the level of prices for buildings in a certain area. To do so, the taxation department re-uses data gathered from registered real-estate sales. Information in environmental fields aimed at informing people about the quality of air or about sounds levels is also offered by re-using data issued from control activities. Mobility information, indicating for example the best combination of train, bus and metro availabilities to reach a point, also needs to re-use information that was not initially offered in shared way and not dedicated to the particular format in which the final information

²³³ See Note (25) of the Introduction to the PSI Directive.

service is delivered. The Estonian Krediidinfo²³⁴ is an example of a company that relies on the re-use of public sector information in its business activities. This company compiles information available in various public sector databases, and in doing so offers its clients one-stop shopping for their information needs. Last but not least, the company adds value to the information collected from the public sector by combining it with private sector information.

Although the PSI Directive has an impact on eGovernment by tackling many related issues, it does not eliminate all obstacles concerning the re-use possibilities of PSI and the establishment of a pan-European public information market.²³⁵ Important rights in this area also need to be re-evaluated if they are not to become obstacles to eGovernment. For instance in the following key areas:

- The PSI Directive leaves to the Member States and their public bodies the determination of whether or not to allow the re-use of public sector information. Hence, there are no guarantees about the re-use of PSI for citizens and businesses.
- As the Directive bases the re-use system on the access regimes of Member States, their implementation vary between Member States, and sometimes between different governance levels within a nation.
- Exceptions exist to re-use permission, for example with some Freedom of Information (FOI) Acts prohibiting certain kinds of re-use of the obtained information. In addition, data protection rules and/or intellectual property rights (IPR) conditions may prevent the re-use of some documents. Furthermore some documents are excluded from the scope of the PSI Directive (e.g. those relating to public sector broadcasters and educational and cultural institutions, including museums.).
- Competition rules that apply to the public sector must be considered in determining whether public bodies may themselves exploit public sector information.
- Technical matters of significance to re-use effectiveness (e.g. a lack of common standards or formats; insufficiently clear information about ways to access public documents in Member States; and no common guidelines for storing such documents).
- Difficulties arising from the need to cater for several languages.
- A lack of clear harmonization regarding charges for the re-use of public documents.

3. What is the European context for this area, including relevant legislation, policy statements, and institutional arrangements relevant to this topic?

The main issues regarding the domain of public sector information have been established for many years²³⁶. The European Commission took its first steps on re-use in 1989 with the (not binding) 'Synergy Guidelines'²³⁷. These sought to strengthen the position of the private sector in the European information market and limit the role of public sector bodies in the supply of raw data. In 1998, a second step resulted in a Green Paper (European Commission 1999) on public sector information. Thereafter, a proposal for a directive was issued that finally resulted in the 'PSI Directive'²³⁸.

²³⁴ See www.krediidinfo.ee and, for a complete analysis, see Open Society Institute (2005).

²³⁵ The European Commission's MEPSIR project has been studying the effects of the PSI Directive on re-use in EU Member States (see <http://www.mepsir.org>).

²³⁶ Relevant publications include: Burkert (1995); Poulet (1996); and de Terwangne, C. (2000). See also the Conference of Stockholm, Access To Public Information: A Key To Commercial Growth And Electronic Democracy, 26 June 1996, and the INFOethics 2000 conference in Paris, 13-15 November 2000.

²³⁷ European Commission (1989).

²³⁸ Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. Actually, the ePSIplus Thematic network (<http://www.epsipius.net/epsipius>) is supporting the implementation of the PSI Directive for the period

As highlighted in its Recital 25, the objectives of the PSI Directive are primarily :

“ to facilitate the creation of Community-wide information products and services based on public sector documents, to enhance an effective cross-border use of public sector documents by private companies for added-value information products and services and to limit distortions of competition on the Community market ”.

It was also considered that this could not “be sufficiently achieved by the Member States and [would] therefore, in view of the intrinsic Community scope and impact of the said action, be better achieved at Community level”. On the basis of the Subsidiarity Principle of Article 5 of the Treaty of Amsterdam²³⁹, the Community took action in this domain. However, this was limited by the principle of proportionality set out in the same article.

Another reason for the limited European harmonization in this domain include those cited by Prins (2005): “The remains of the political struggle and lobbying of different organizations are apparent when looking at the actual scope of the final directive. Here, the ambitious initiative to regulate the European information market is considerably mitigated. Various public sector documents that are in principle of high interest for the private sector are left outside the ambit of the regulatory regime.”

At the European level, Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, was also adopted to “give the fullest possible effect to the right of public access to documents” and to “improve the transparency of the decision-making process” by the European institutions. Other texts²⁴⁰ were also adopted in order to increase the right of access to EU documents (« not only to documents drawn up by the institutions, but also to documents received by them, in all areas of activity of the European Union »²⁴¹) and their re-use by others.

The re-use legal landscape in Europe is therefore made of a patchwork of legal layers that can get entangled with each other. The upper (European) layer is built on the access to public information regimes allowed within the lower layers in Member States and the specific re-use rules applicable at national, regional, state or local levels.

4. What is the relationship of the Re-Use of Public Sector Information to the seven barrier categories and associated research questions?

4.1 Leadership failures (significant)

The PSI directive does not impose the re-use faculty. It only seeks to ensure that in cases where re-use is admitted, EU Member States follow a harmonized implementation framework. The decision to allow re-use of PSI depends on the policy of each Member State. Most EU countries do not have a global policy in terms of re-use of PSI. In the vast majority of situations, re-use possibilities rely on the initiatives and willingness of persons

leading up to its review in 2008, and provides a ‘one-stop shop’ for key information on PSI re-use across European Union.

²³⁹ The Subsidiarity Principle states: “it is the principle whereby the Union does not take action (except in the areas which fall within its exclusive competence) unless it is more effective than action taken at national, regional or local level. It is closely bound up with the principles of proportionality and necessity, which require that any action by the Union should not go beyond what is necessary to achieve the objectives of the Treaty” (http://europa.eu/scadplus/glossary/subsidiarity_en.htm). This Principle was introduced in the EU Amsterdam Treaty, agreed by the European Union's political leaders on 17 June and signed on 2 October 1997.

²⁴⁰ See European Commission (2001); the Commission Initiative ‘i2010 – a European Information Society for growth and employment’; and European Commission (2006).

²⁴¹ See Recital 10 and Article 2 (3) of Regulation 1049/2001.

holding the regulatory power inside an administrative department or a public entity. In such cases, leadership failures have a significant impact in this area.

The Mepsir (2006) Final Report has recently stressed in its conclusions that :

“there still exist a considerable gap between the current ‘baseline’ situation and the one sought by the Directive. We expect that the Directive will have its effect on the economic performance in the value chain soon, whereby the various indicators, such as transparency and accountability and non-discrimination will serve as ‘leads’ and the market results as ‘lags’”²⁴².

4.2 Financial inhibitors (very significant)

In the past, there have been problems linked to too high a price being asked to allow interested persons to re-use PSI. The adoption of the PSI Directive should have solved those. Indeed, charges now normally fixed for the re-use of PSI must be cost-oriented and include a reasonable return on investment. Such charges should not therefore be a financial inhibitor for actors interested in developing information products on the basis of available PSI.

It can already be said that onerous charges can follow from the political choice to allow public sector entities to include costs of collection and production in the charges imposed for re-using PSI. We can also note that the too blurred notion of “reasonable return on investments” could lead to remaining financial inhibitors in the re-use of PSI.

This is particularly true in areas where competition exists between public interests and private ones. Competition notably arises in situations where a public entity (like a statistical institute or a national geography institute) is asked to find external funds to support its activities financially. In such cases, the public entity is tempted, or even obliged to, develop informational by-products.

It appears that problematic situations are likely to arise:

- When the public entity asks for too high charges to allow private entities to receive PSI and develop new informational products or services based on the received information. This excludes most of the private possible competitors and leaves the public entity dominate the concerned market segment. Article 8 of PSI Directive normally prevents such behaviour²⁴³.
- When the public entity sells its informational services at prices lower than market prices (to exclude private sector competitors). This is a problem for private sector entities willing to offer similar products. If the new informational product or service is considered as answering to a general interest and falls under public service category, the public entity is justified to act so; but if it is not the case, the public entity must respect competition rules and avoid cross-subsidiary financing between its public tasks and the new service not considered as a public task. Article 10.2. of the PSI directive offers an answer to this possible problem²⁴⁴.

²⁴² Mepsir (2006), pp.45-54.

²⁴³ Article 8 states that : “Public sector bodies may allow for re-use of documents without conditions or may impose conditions, where appropriate through a licence, dealing with relevant issues. These conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.” (author has added underlining)

²⁴⁴ Article 10 on « non-discrimination » states : “2. If documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the documents for those activities as apply to other users”.

- When the public entity sells its informational products at high market prices (if it is in a quasi-monopolistic position and does not fear any serious competitor). This is a problem for the service end-user.

Results from the MEPSIR (2006) study²⁴⁵ has shown that reality does not correspond to this ideal yet. In fact, in its conclusions (see previous point) it mentions that the PSI Directive “will bring” (so has not yet brought) a ‘direct price effect’, as the “costs of purchasing public sector information from the government will decrease”, and a ‘fading price effect’, as “this lowering of costs is (partly) translated into lowered prices in the successive parts of the chain”.

4.3 Digital divides and choices (significant)

Re-use of public sector information can be hindered by a lack of transparency about re-use possibilities and related practical issues that can benefit or disadvantage different sections of society. Article 7 of the PSI Directive²⁴⁶ imposes transparency and is thus expected to solve this problem.

To offer information easily re-useable, documents need to be provided in formats that can be easily accessed by a wide range of potential users. Article 5 of the PSI Directive suggests a principle of delivery in electronic format “where possible and appropriate”, but with no obligation to create or adapt documents, nor to provide extracts where this would involve “disproportionate efforts”.

Due to the diversity of its Member States, a major obstacle to eGovernment developments in EU can be the need to make available public documents in languages of other Member States and in ways that can be understood by citizens/businesses or public bodies of other Member States.

Another potential barrier is the lack of common principles and guidelines for storing PSI.

4.4 Poor coordination (very significant)

The PSI Directive is substantially limited as a tool for harmonizing regulation of the re-use of public sector information. It leaves detailed regulation to the Member States and their public bodies, which means there is no overall guarantee in the EU regarding such re-use.

For example, Article 6 of the PSI Directive has an imprecise reference to “a reasonable return of investment” when fixing charges for the re-use of public documents, which does not provide sufficient clarity as a harmonizing guideline.

For instance, this is illustrated by the Federal Belgian FOI law of 11 April 1994²⁴⁷, which states: “The administrative documents obtained in the framework of the present law may not, for commercial purposes, be broadcasted, distributed, nor re-used”²⁴⁸.

²⁴⁵ The European Commission’s MEPSIR project has been studying the effects of the PSI Directive on re-use in EU Member States (see <http://www.mepsir.org>)

²⁴⁶ Article 7 on “transparency” states : “Any applicable conditions and standard charges for the re-use of documents held by public sector bodies shall be pre-established and published, through electronic means where possible and appropriate.”

²⁴⁷ See www.privacyinternational.org/countries/belgium/loi-publicite.rtf for more information on the Belgian Federal FOI Law of 11 April 1994 ‘Relative à la Publicité de l’Administration’.

²⁴⁸ Free translation of Article 10 of the Belgian Federal FOI Law of 11 April 1994 relating to the publication of information by the administration. In Belgium, certain regulations at regional level severely punish as a penal offences the non-observance of a prohibition that is present at regional level.

Despite a reliance on the access regimes of Member States, a common theme on PSI re-use exists to a certain extent through the principles laid down in Recommendation R(81)19 of the Council of Europe of 25 November 1981, which has been taken as a model by many Member States²⁴⁹.

Other rules regulating specific areas at national, regional or even local level may also have to be taken into account when addressing the question of re-use of PSI in order to develop eGovernment services or products. For instance, in most European Member States, there is one central body that collects information on companies, as exemplified by the IT Consortium of Italian Chambers of Commerce (InfoCamere²⁵⁰), the Belgian 'Banque-Carrefour des Entreprises'²⁵¹ (Crossroad-Bank of Enterprises) and the Hungarian Company Registry and Information Service²⁵². These bodies centralize detailed information on all the firms in the country, including legal status, registration details and balance sheets. This offers a single location for anyone seeking information about a company, or a company wanting to license this information

Nevertheless, other European countries do not follow this centralized model. As Pira International (2000) explains: "In Germany companies do not register centrally but with their regional authorities. Hence companies wanting to exploit this information (such as directory publishers or credit information providers) need to contact all the individual regional authorities. In Greece the situation is even more difficult with no government department collecting companies information. This means that any organization wanting to publish information on Greek companies needs to get the information directly from each individual company".

4.5 Workplace and organizational inflexibility (significant)

A lack of a PSI re-use culture persists in Member States. The adoption of the PSI Directive has begun to change the situation, but only gradually and patchily²⁵³.

Some public sector documents are explicitly excluded from the scope of the PSI Directive in its Article 1 (2), which determines also that its regime is not applicable to documents that form part of an activity falling outside the scope of the public task of the public sector bodies. Therefore, in applying the PSI Directive, it is very important to determine what is and is not a 'public task'.

4.6 Lack of trust (significant)

Private sector has generally the impression that there is no "independent" counterpart against the "all-powerful" public bodies regarding the public sector information on their own, as they can unilaterally decide what is or not within their "public task" and exclude some re-use at all. Even if the Article 4(4) of the PSI Directive states that "any negative decision shall contain a reference to the means of redress in case the applicant wishes to appeal the decision", there is clearly a lack of transparency to simplify the appeal procedures in the practice, and private stakeholders still have the impression that nothing is done to change that established fact²⁵⁴. As it was underlined by the ePSIplus Network

²⁴⁹ See Section 5.6 on "Public Administration Transparency".

²⁵⁰ See: <http://www.infocamere.it>

²⁵¹ See: <http://kbo-bce-ps.mineco.fgov.be>

²⁵² See: <http://www.im.hu>

²⁵³ As it was noticed by Ireland, for instance, in the 9th Meeting of the PSI Group, held in Luxembourg on 28 November 2006, there is still a "need for additional efforts on awareness and promotion of re-use (supply and demand)".

²⁵⁴ This was many times stressed by participants on recent EPSIplus Thematic Meeting "PSI Pricing 1: Impact Analysis in the Context of the PSI Directive", held at Helsinki on 19-20 April 2007.

“the private sector is [still] inclined to be cautious and risk-averse when it comes to dealing with public sector bodies and building businesses and services based on PSI”²⁵⁵.

Moreover, there are often no general guidelines at the national level (translated by a lack of transparency of public administration “obligations”) and specially a lack of awareness regarding the PSI re-use economic opportunities.

In the UK, the Office of Public Sector Information (OPSI)²⁵⁶ is a good example of the re-organization of services to meet the requirements of the PSI Directive: it is an “independent” body at the heart of the UK information policy, which sets standards and provides a practical framework of best practices for opening up and encouraging the re-use of public sector information. It has also an important role as a regulator of public sector information holders for their information trading activities, and has the power to investigate complaints against public sector information holders made under the Re-use of PSI Regulations.

4.7 Poor technical design (significant)

There are problems of re-usability in relation to document formats. Offering public information for re-use purposes does not necessary imply that this information is easily re-useable. For this, documents need to be provided in formats that can be easily accessed by a wide range of potential users. At the same time, public services should not be expected to support unacceptably high new administrative and financial burdens in order to support any reformatting necessary to achieve this. Article 5 of the PSI Directive suggests a principle of delivery in electronic format “where possible and appropriate”, with no obligation to create or adapt documents nor to provide extracts where this would involve disproportionate efforts. Reference is also made in Recital 13 to the need for conformity to technical open standards to ensure wide accessibility, at least at a technical level.

5. What are the barriers remaining in this field?

5.1 Lack of a European culture of PSI re-use

In its brochure on exploiting the potential of Europe’s PSI, the European Commission (2004) states: “The re-use of public sector information is a relatively new topic. With the Internet, the potential of this information as an economic asset has grown exponentially. This potential is, however, not widely identified within the public sector. There is at present no culture of systematically taking into account the possibility of re-use. It will take some time before such a culture develops throughout Europe”. As already mentioned, progress towards this is being supported by the PSI Directive but much still needs to be done. For example, in the relatively under-developed market of environmental information, obstacles are often caused by public suppliers who are not accustomed to locating appropriate information or negotiating with the private sector²⁵⁷.

Even if at present some actions are conducted at the European level to overcome this barrier²⁵⁸, the commercial re-use of PSI is always insufficiently exploited by private sector and by public bodies themselves, by comparison with their US counterparts for instance.

²⁵⁵ See ePSIplus Newsletter of 1st January 2007 on http://www.epsiplus.net/epsiplus/news/newsletter/epsiplus_update_no_1.

²⁵⁶ See: <http://www.opsi.gov.uk/>.

²⁵⁷ Example cited in Pira international (2000).

²⁵⁸ See, for instance, the actions undertaken by the ‘PSI Group’, an expert group initiated by the European Commission to discuss transposition issues and to stimulate the exchange of good

Related barriers: workplace and organizational inflexibility, poor coordination

5.2 Exclusion of some documents

As previously indicated, some public sector documents are excluded from the scope of the PSI Directive, such as those for which third parties hold the IPR or documents excluded from access by virtue of the access regimes in the Member States²⁵⁹. In addition, Article 1(2a) of the Directive determines also that its regime is not applicable to documents that form part of an activity falling outside the scope of the public task of the public sector bodies.

This indicates why it is very important when applying the PSI Directive to define what is a 'public task'²⁶⁰. It could be seen as a task that is directly related to the core activity of a public body, as opposed to an optional commercial product competing in the open market. But it is not always easy to identify directly what should be considered as 'related tasks' (e.g. in order to offset overhead costs, government trading funds may be employed to develop profitable commercial outlets for public administrations' services, which are often built around information provided as part of public task). However, this does not mean that everything produced by public bodies falls within the definition of a public task in relation to the PSI Directive.

The differences and uncertainties that exist between Member States regarding the basic definitions can create difficulties for EU citizens and enterprises in understanding a specific legal framework (e.g. knowing beforehand which re-use activities are worth introducing). Public administrations, on the other hand, may have difficulties in knowing exactly which documents – or part of documents – they are allowed to re-use.

Related barriers: poor coordination, workplace and organizational inflexibility

5.3 Obstacles related to IPR²⁶¹

The PSI Directive has not solved the problem of divergences of national legal regimes regarding IPR or the absence of such rights for certain government documents. No existing intellectual property rights are affected by the PSI Directive.

The obstacles posed by IPR to accessing protected documents, such as providing an exemption to access rights, can be even more severe in relation to the re-use of public documents. For instance, although the holding of IPR on certain documents by public administrations may not prevent access to those documents, obtaining the right to re-use such documents could be much more difficult and more expensive than in the private sector. As a minimum, IPR requires obtaining the consent of the owner of the rights, and in many cases to pay or buy a license to re-use the documents.

practices between Member States, and the co-financing projects by the EC aiming especially to bring out the potential of PSI (http://ec.europa.eu/information_society/policy/psi/actions_eu/index_en.htm), as the ePSIplus Network, which foresees thematic meetings on PSI Culture to reinforce awareness on it

(http://www.epsiplus.net/epsiplus/events/epsiplus_thematic_meetings/public_sector_culture_thematic_meetings).

²⁵⁹ In fact, Article 1 (2) c) of PSI Directive states that: "[this Directive shall not apply to] documents which are excluded from access by virtue of the access regimes in the Member States, including on the grounds of : the protection of national security (...) [and] statistical or commercial confidentiality".

²⁶⁰ See for instance the OPSI (UK) Statement in relation to APPSI review (2007), where we can see how much difficult it is to agree to a common definition of a "public task", even for two "independent" bodies. See also its definition of a "public task" of a PSI Holder (OPSI 2006, p.7).

²⁶¹ See also Section 5.3 on IPR.

Related barriers: poor coordination

5.4 Data protection requirements²⁶²

The data protection legal framework has an effect on the re-use of electronic public sector documents in that the PSI Directive cannot over-ride the protection of individuals with regard to the processing of personal data²⁶³. Thus, even if re-use is generally accepted in a Member State, it can be refused in a specific case on the basis of data protection rules. For instance, if a re-use purpose is not compatible with the initial administrative purpose for which the personal data has been collected, re-use cannot be accepted without the agreement of the person concerned.

Such a barrier to re-use and to the take up of certain kinds of eGovernment services and products is justified by the concern for protecting other important interests, i.e. the data subject's interests in controlling data relating to him/herself and in avoiding incompatible uses of data. The aim should not be eliminate this, but to balance these interests with other factors affecting eGovernment outcomes.

Related barriers: poor coordination

5.5 Competition between public and private interests

Competition between public interests and private ones is an important consideration in relation to PSI re-use. The difference between raw and added-value data when in electronic form is small, and public bodies are often tempted to exploit their information to gain revenue for themselves. Competition rules will not necessarily prevent public bodies from doing this, although they have an important influence on the entrance of some public or private actors in the re-use arena. For example, Pira International (2000) notes: "the main obstacle for companies working in the well-developed market of companies information may be potential competition from the public sector itself and the price it wants for the data".

A first step already mentioned is to determine where the public bodies are acting within – or outside – the framework of their public mission. Another important issue is the application of the re-use legislation. For instance, what exactly is meant in the PSI Directive by the use "for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced?"²⁶⁴. Does this indicate that the re-use legislation will be applicable as from the moment of the existence of a slight difference between the "re-use" purpose and the initial one, or should the purposes be completely different? Even when we are talking about an eGovernment service determined in the framework of the public mission of a public body, the re-use legislation can be applicable if we are outside the field of the initial purpose. However, this will not be easy to determine.

Public bodies must also refrain from giving exclusivity rights to certain partners or to themselves regarding PSI re-use, and must also avoid cross-subsidiary of their commercial activities. In Sweden for instance, "there is an inadequate separation of commercial activities from public governance and public service functions of public agencies operating on a commercial scale"²⁶⁵.

²⁶² See also Section 5.5 on Privacy and Data Protection

²⁶³ Article 1(4) of the PSI Directive.

²⁶⁴ Article 2(4) of the PSI Directive.

²⁶⁵ Knut Rexed, Director General of the Swedish Statskontoret, 5th Meeting of the Public Sector Information Group, Luxembourg, 23 April 2004.

In the UK, the Office of Public Sector Information (OPSI)²⁶⁶ is at the heart of information policy, setting standards and providing a practical framework of best practice for opening up and encouraging the re-use of public sector information. It offers a wide range of services to the public, the information industry, government and the wider public sector relating to finding, using, sharing and trading information.

As we have mentioned before, OPSI is a good example of the re-organization of services to meet the requirements of the PSI Directive. For instance, as stated in ePSINet (2004):“OPSI has : improved dissemination of PSI and services to citizens and business; it provides quick and easy access to data; established good public/private sector co-operation; created more effective, relevant and permanent links and thus enhanced interoperability by improving the distribution of information across a variety of media, systems and different government departments; launched the online ‘Click-Use’ Licenses which allow unrestricted use of government information. These standard licenses facilitate PSI exploitation by removing conflicts and simplifying negotiation between public bodies and private operators; publishes license terms and conditions, transparent pricing structure for the re-use and reply time; prohibits exclusive arrangements which hamper fair competition; has made digital format the primary form of dissemination; allows access to any pre-existing format; developed and adopted common standards and metadata; publishes electronic catalogues of accessible data resources and has created the ‘Inforoute’ portal which is linked to decentralized assets lists; publishes how to complain or appeal if re-users feel that they have not been treated fairly”.²⁶⁷

Comparisons of OPSI with other similar bodies illustrates, on one hand, the interesting harmonization brought by the PSI Directive. But it also points to difficulties created by remaining divergences between Member States on PSI re-use, particularly for the development of cross-border or pan-European information products or services. For instance, the French public service organization (SPDDI) providing law diffusion via the Internet has to make essential legal norms and case-law freely available for Internet users. The Légifrance website was created for this purpose²⁶⁸. The re-use rules set out in the PSI Directive are met by both Légifrance (notably the transparency requirements) and OPSI. This illustrates how certain obstacles to re-use addressed by the Directive can be overcome.

However, the rules adopted to allow the re-use of published public sector information vary between different contexts. For example, Légifrance states that all the databases accessible through its website are protected under provisions of Title IV of Book III (Article L.341-1) of the French Code of Intellectual Property. This requires that every extraction or re-use of “quantitatively or qualitatively substantial parts of the content” of one of the databases supposes the previous conclusion of a license to allow that re-use. The Légifrance website explains what is meant to be perceived by terms such as quantitatively substantial and qualitatively substantial. Therefore, a user who does not intend to re-use such substantial parts may freely re-use almost everything contained in the French databases because most of these legal data are not covered by copyright protection. OPSI policy, on the other hand, is different. Most UK legal material is covered by Crown copyright, which means that a check has to be made of the items published on the OPSI website to determine whether a license is needed for re-use or whether the person accessing the information falls into a listed exemption category.

The Hungarian Official Journal publisher manages a database on Hungarian laws, decrees, court decisions and other administrative rulings dating back to 1991. It is available in different versions and formats (CD-ROM, DVD and online). Whereas this case²⁶⁹ is quite similar to the ones mentioned above, it presents certain specificities: the Publisher does not provide free access to Hungarian legislation, with all printed, electronic

²⁶⁶ Previously Her Majesty's Stationary Office (HMSO).

²⁶⁷ ePSINet (2004).

²⁶⁸ See: <http://www.legifrance.gouv.fr>

²⁶⁹ See a complete presentation of this case in Open Society Institute (2005).

and online publications are charged for independently of whether they contain raw or value-added material; and full catalogues of all publications are available for sale.

An example from Latvia is Lursoft IT Ltd²⁷⁰, which is in charge of developing a Court Information System for the Latvian Ministry of Justice, including a Database of Decisions of the Supreme Court. Access to this 'Database of Court Judgements' takes place against a fee.

Finally, in the same field of dissemination of legal information the examples of the Service Centre of the Chancellery of the Prime Minister (COKPRM)²⁷¹ and the Supreme Administrative Court (NSA)²⁷² in Poland are illustrative of the ineffectiveness of PSI directive. The activities of these entities have only partially meet the Directive. The main obstacles to an appropriate implementation of the Directive hereby are as follows:

- "Lack of clear policy for an effective dissemination of legal information in Poland. There is no single access point where most of binding law and case legislation could be obtained free of charge.
- Rather limited access to material online. It is also not really user friendly.
- Insufficient information about the conditions of the re-use and time of reply²⁷³.

Related barriers: poor coordination, workplace and organizational inflexibility

5.6 Charges for re-use

The reference in Article 6 of the PSI Directive to "a reasonable return of investment" when fixing charges for the re-use of public documents is too imprecise to form a basis for consistency across Member states.

However, the Directive imposes conditions of publicizing the kind of information that need to be provided to explain the terms under which PSI is available for re-use. For instance, despite the official implementation of the PSI Directive in Italy, InfoCamere does not comply with the Directive requirement as pricing conditions for re-using information contained in its data bases are not available on its website²⁷⁴.

Furthermore, the PSI Directive authorises now charges for costs of "reproduction and dissemination" as well as costs of "collection and production"²⁷⁵ of documents, which could rapidly increase the costs for private sector in some crucial fields (such as meteorological sector, for instance²⁷⁶) and that, in practice, constitutes a clear misuse of power of the public sector regarding the determination of such costs. One should stress the fact that the PSI Directive is rather contradictory about that issue, as in its Recital (14) it states, on the other hand, that "(...) Member States should encourage public sector bodies to make documents available at charges that do not exceed the *marginal costs for reproducing and*

²⁷⁰ See: www.lursoft.lv

²⁷¹ See: <http://www.cokprm.gov.pl>

²⁷² See: <http://www.nsa.gov.pl>

²⁷³ Open Society Institute (2005).

²⁷⁴ For a detailed description of the InfoCamere case, see <http://www.infocamere.it> and ePSINet 2004 (the description presented in this document is still pertinent in December 2006).

²⁷⁵ In fact, article 6 of the PSI Directives states that: "where charges are made, the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment (...)"

²⁷⁶ See, for instance, the sample of the "European Weather data pricing" presented by Dr. Pirkko Saarikivi, from FORECA Limited of Finland, at the ePSIplus Thematic Meeting about "PSI Pricing: Impact Analysis in the context of the PSI Directive, Helsinki, 19-20 April 2007.

*disseminating the documents*²⁷⁷. This is a relevant issue, which has to be clarified in an eventual future revision of PSI Directive.

For instance, the MEPSIR (2006) survey provides a useful base line for testing the trends with respect to charging and it invites national experts to workshops, as those organised by ePSIplus Thematic Network, in order to clarify the situation at a cross-border level.

Related barriers: digital divides and choices, poor coordination

5.8 Identifying the availability of documents

In a highly fragmented arena such as the public sector, it is difficult to know precisely what information is available for re-use. Article 9 of the PSI Directive refers to the need for practical arrangements to facilitate the search for available documents. An important organizational obstacle to eGovernment could arise if there is no clear, easily accessible and understood information for all citizens of all the Member States about, for instance, the way to obtain information, the availability of information and the conditions under which such information can be accessed for re-use in every Member State. Without such information on re-use availability, regimes for cross-border or even national access and re-use regimes are likely to be ineffective.

The OPSI and French Légifrance services are examples of good practice in this respect, as they offer lists of information available for re-use together with simple 'click and use' methods to agree any necessary license to enable appropriate re-use.

Related barriers: leadership failures, digital divides and choices, poor coordination

5.9 Language diversity

As already mentioned, due to the diversity of its Member States a major obstacle to eGovernment developments in Europe can be the need to make available public documents in languages²⁷⁸ of other Member States. As Prins (2005) observes: "Language diversity represents a challenge to the pan-European exploitation of public sector information. The costs involved in the translation of the raw material and the need for linguistic customization of the added-value end product is an additional difficulty that has to be overcome by information companies that want to step into this market"²⁷⁹.

Related barriers: digital divides and choices, poor coordination

5.10 Common standards for storing public sector information

Despite a lack of common principles and guidelines for storing PSI, which could be a significant potential eGovernment barrier there are examples of successful integration of data within one Member State. One is the MIDAS system in use in the Czech Republic, a public-private partnership that has operated since 2000 to provide a description and overview of existing data in the area of geographic information. It helps to co-ordinate data requirements, share data and remove duplication of efforts. The MIDAS free portal

²⁷⁷ The same solution was adopted by European Commission in its Decision of 7 April 2006 on the re-use of Commission information (2006), which states in Article 7: "the re-use of documents shall in principle be free of charge. In specific cases, marginal costs incurred for the reproduction and dissemination of documents may be recovered".

²⁷⁸ There are currently 23 Official Languages within the EU (see ePSIplus 2007b, p.9).

²⁷⁹ European Commission (2001).

website²⁸⁰ gives access to a large number of datasets drawn together from different sources within a common standard (see also European Commission 2004).

Related barriers: leadership failures, digital divides and choices, poor coordination

Sources

Publications

- Burkert, H. (1995), 'Public Sector Information: Some Implications for a European Information infrastructure', KnowRight 1995, 133 – 138
- de Terwangne, C. (2000), *Droit à l'Information et Droit à la Transparence. Vers Une Europe de la Connaissance?*, Doctorate Thesis, University of Namur, Belgium.
- ePSINet (2004), *Practices of Exploitation of PSI: Deliverable related to WP2 Task 4 in the framework of the EPSINet Project*, Florence and The Hague: ePSINet, 25 August, <http://www.epsigate.org>
- ePSIplus (2007a), *Public Sector Information: A collation of country reports provided by the Thematic Network Partners*, V2.1, 24th February 2007, 88 p., http://www.epsiplus.net/epsiplus/media/files/epsiplus_countryreports_24feb07_v2_1
- ePSIplus (2007b), *Public Sector Information: Financial impact of the PSI Directive – Pricing and Charging Key Issues – An overview*, V2.0, 15th April 2007, 61p., http://www.epsiplus.net/epsiplus/media/files/epsiplus_pricingintroduction_v2
- European Commission (1989), *Information Industries and Innovation: Guidelines for Improving the Synergy between the Public and Private Sectors in the Information Market*, Brussels: Directorate-General for Telecommunications.
- European Commission (1999), *Green Paper on Public Sector Information in the Information Society*, COM (98) 585 Final, adopted on 20 January 1999, Brussels: European Commission, [http://europa.eu.int/ISPO/docs/policy/docs/COM\(98\)585/gp-chapter3.html](http://europa.eu.int/ISPO/docs/policy/docs/COM(98)585/gp-chapter3.html)
- European Commission (2001), *Communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, 'eEurope 2002: Creating a EU Framework for the Exploitation of Public Sector Information'*, 23 October, COM (2001) 607 final, Brussels: European Commission, http://europa.eu.int/information_society/europe/2002/news_library/new_documents/public_sector/public_sector_en.pdf
- European Commission (2004), *Exploiting the Potential of Europe's Public Sector Information*, Brussels: Directorate General for the Information Society, Unit Information market (E4), May, http://europa.eu.int/information_society/policy/psi/library/index_en.htm#4.%20Brochure%20PSI%204
- European Commission (2006), *Decision of 7 April 2006 on the re-use of Commission information*, (2006/291/EC, Euracom), OJ L107, 20.4.2006, p.38, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_107/l_10720060420en00380041.pdf
- MEPSIR (2006), *Final Report on Study on Exploitation of PSI – benchmarking of EU framework conditions*, June, http://www.epsiplus.net/epsiplus/reports/mepsir_measuring_european_public_sector_resources_report
- Open Society Institute (2005), *Case Studies on Regulatory Impact*, ePSINet CEE Project, Deliverable D.4.1, Budapest, 15 April, <http://www.epsigate.org/>

²⁸⁰ See: <http://www.cagi.cz/midas>

OPSI (2006), Report on its investigation of a complaint (SO 42/8/4): Intelligent addressing and Ordnance Survey, July 2006, <http://www.opsi.gov.uk/advice/psi-regulations/complaints/SO-42-8-4.pdf>

OPSI (2007) Statement in relation to APPSI review: Intelligent Addressing and Ordnance Survey, 30th April 2007, <http://www.opsi.gov.uk/advice/psi-regulations/complaints/statement-review-SO-42-8-4.pdf>

Pira International (2000), Commercial Exploitation of Europe's Public Sector Information, e Content – Spice Preparatory Action II, Final Report, 30th October, ftp://ftp.cordis.europa.eu/pub/econtent/docs/commercial_final_report.pdf

Prins, J. E. J. (2005), Commentary on Directive on the Re-use of Public Sector Information, in Büllsbach, A., Pouillet, Y. and Prins, C (eds), Concise Commentary on European IT Law, Kluwer Law International, Alphen aan den Rijn.

Pouillet, Y. (1996), Plaidoyer pour un ou des Service(s) Universel(s) d'Informations Publiques, Access To Public Information: A Key To Commercial Growth And Electronic Democracy, Conference of Stockholm, 26 June, <http://europa.eu.int/ISPO/legal/stockholm/welcome.html>

International and European-level Legislation, Regulations, Conventions and Treaties

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, Official Journal L 345, 31/12/2003, pp. 0090-0096, http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_345/l_34520031231en00900096.pdf

Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, Official Journal L 143, 31.5.2001, pp. 43-48, http://www.europarl.europa.eu/register/pdf/r1049_en.pdf

Recommendation R(81)19 of the Committee of Ministers to Member States on the Access to Information Held by Public Authorities, adopted by the Committee of Ministers on 25 November 1981 at the 340th meeting of the Ministers' Deputies, [http://www.coe.int/T/e/legal_affairs/Legal_co-operation/Administrative_law_and_justice/Texts_&_Documents/Recommendation\(81\)19.asp](http://www.coe.int/T/e/legal_affairs/Legal_co-operation/Administrative_law_and_justice/Texts_&_Documents/Recommendation(81)19.asp)

EU Amsterdam Treaty of 2 October 1997, <http://europa.eu/scadplus/leg/en/s50000.htm>

Websites

eContentplus Programme, adopted on 9 March 2005 by the European Parliament and the Council, a multiannual Community programme to make digital content in Europe more accessible, usable and exploitable, http://ec.europa.eu/information_society/activities/econtentplus/index_en.htm

European Commission, Directive on PSI re-use: list of notified transpositions by Member States, http://ec.europa.eu/information_society/policy/psi/actions_ms/implementation/index_en.htm

European Commission, Initiative 'i2010 – a European Information Society for growth and employment', http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm

Conferences, workshops, etc relevant to eGovernment

- Conference of Stockholm, Access To Public Information: A Key To Commercial Growth And Electronic Democracy, 26 June 1996,
<http://europa.eu.int/ISPO/legal/stockholm/welcome.html>
- INFOethics 2000 conference, Paris, 13-15 November 2000,
<http://webworld.unesco.org/infoethics2000/>
- 9th Meeting of the PSI Group, held in Luxembourg on 28 November 2006,
http://ec.europa.eu/information_society/policy/psi/news/index_en.htm
- EPSIplus Thematic Meeting: PSI Pricing 1: Impact Analysis in the Context of the PSI Directive, Helsinki, 19-20 April 2007,
http://www.epsiplus.net/epsiplus/events/epsiplus_thematic_meetings/financial_impact_thematic_meetings/psi_pricing_1_impact_analysis_in_the_context_of_the_psi_directive

Research projects relevant to Re-use of PSI legal issues

- ePSINet (the European Public Sector Information Network), supports cohesive approaches towards Public Sector Information in Europe. It develops knowledge-sharing relationships with and between sectoral organizations, while building international co-operation with the USA and other countries, (see <http://www.epsigate.org>).
- ePSIplus, which is a Thematic Network, funded by the European Commission under the eContentplus programme to support the implementation of the PSI Directive in the period leading up to its review in 2008. It is a “one-stop shop” for key information on PSI re-use across Europe and includes news, reports, legal cases, good practices and benchmarking on the progress of legislation of Member States (see <http://www.epsiplus.net/epsiplus>).
- MEPSIR, a European Commission study that defines, tests and applies a methodology to measure the re-use of PSI in EU Member States, serving as a basis for the review of Directive 2003/98/EC three years after its implementation (see <http://www.mepsir.org>).
- OECD Working Party on the Information Economy (WPIE) work programme on digital broadband content studying scientific publishing, music, online computer and video games and mobile content, including reviewing, assessing and developing good practice guidelines on government practice in making public sector information and other content more accessible, (see www.oecd.org/sti/digitalcontent).