



E-GOVERNMENT AND TELECOMMUNICATIONS

TABLE OF CONTENTS

- I. INTRODUCTION**
- II. E-GOVERNMENT**
- III. TELECOMMUNICATIONS**
- IV. SPAM**
- V. CONCLUSIONS**

I. INTRODUCTION

The Information and Knowledge Society has brought profound changes in its wake throughout the world. This transformation is fuelled primarily by the appearance of the new media now available that create and spread information and knowledge through information and communications technologies (hereinafter, ICT). Thus, new forms of social and productive organisation have emerged, as well as a new culture. The means of communicating, working and setting up our organisations and communities have changed. We are all witnesses to this process of globalisation, which has altered our concepts of space and time and done away with existing borders. However, we each live these transformations in different ways, depending on economic development, the type of insertion, culture, and strengths and weaknesses of the institutions existing in the various national communities. For our countries, it is vital to determine how this paradigm can contribute to attaining farther-reaching developmental goals that encompass sustainable economic growth, greater equality and a wider spread of democracy, and how to guide our Region wisely into the world information society.

Moving forward toward an information society that benefits all the inhabitants of the Region and promotes the goals set out above requires a continual dialogue that enables us to embark on an agenda able to speed up the process and reduce its economic and social costs. Hence, strategies for the development of the information society that go far beyond national borders must be designed and will make cooperation between countries essential.

The similarity between the challenges involved in ICT's and data protection gives us the opportunity to implement measures designed to enhance the national strategies undertaken to speed up a process of development aimed at social cohesion and inclusion of all members of society.

Within this framework, we will deal with topics such as e-government, personal data processing in telecommunications and, in particular, relatively recent phenomena such as "*spam*".

In this context, the guarantees inherent in the fundamental right to personal data protection in the use of the new technologies acquire enormous relevance and make it essential that we find alternatives that prevent violations of this right, given the myriad of ways in which the public's data may now be used.



E-GOVERNMENT AND TELECOMMUNICATIONS

The concept of security has also taken on significant importance and is closely linked to purpose and consent. It is thus that the suitable degree of security – envisaged in policies, procedural protocols and contingency plans – contributes to attaining the degree of reliability needed to facilitate e-government ventures and due respect for the protection of personal data in the telecommunications sector.

II. E-GOVERNMENT

One of the most complete definitions that covers all the aspects of e-government identifies it as: “The use of information and communications technologies (ICT) by government bodies to better the services and information provided to citizens, to upgrade the efficiency and effectiveness of public management and to substantially increase transparency in the public sector and citizen participation”.

The implementation of e-government is developing gradually, through a process that may be divided into four stages: presence, information, interactivity and transactions.

Suitable development of e-government paves the way for attaining a threefold goal: better citizens’ services, good government and the expansion of democracy. These three areas may be analysed as follows:

Better citizens’ services encompass the establishment of new relationships between government-citizens-companies-investors, through the use of information and communications technologies that allow the State to provide its services efficiently, effectively and independently of physical location.

Good government seeks to establish and introduce new internal methods and processes in State Government that enable the systems from all the different services to integrate, share resources and optimise their internal operation.

The expansion of democracy involves the creation of mechanisms that allow citizens to play a proactive role in the day-to-day operation of the country through the use of information and communications technologies, which afford new areas and forms of participation.

The importance of the aforesaid goals and the fact that the State has a direct relationship to all citizens make furthering e-government projects a priority, as these initiatives have a catalysing and fuelling effect on the digital economy and the information society.



E-GOVERNMENT AND TELECOMMUNICATIONS

Moreover, these areas – better citizens' services, good government and the expansion of democracy - all involve regulatory, organisational and technological components.

Thus, the integration of ICT's must follow a strategic plan that envisages the legal and technological aspects from an interdisciplinary perspective and seeks to facilitate such integration and promote an environment of security.

The existence of a previously defined legal framework is fundamental in creating and providing guarantees that fall within the parameters of technological neutrality from the very outset of these processes.

Sharing of information within the public administration is increasingly important in these modernisation processes and the progress made in e-government, aimed at reaching a degree of inter-operability that eliminates reiterative data requirements for citizens who process accessible non-confidential information within the confines of the authority and powers of the government institutions. Access to confidential data must be subject to specific restrictions defined according to the scenario existing in each country. In this respect, the fundamental right to personal data protection must be reaffirmed, and thus, government must act in accordance with the guarantees inherent in a Rule of Law.

With regards to technological requirements, it is important to highlight the problem of identification and authentication of citizens. In this area, the development of systems that enable the incorporation of services such as digital signature, with the proper guarantees, is enormously useful. Moreover, policies must be established on the security and confidentiality of data, and must envisage a guaranteed supply of electricity, the suitable location of equipment and systems, controlled access that allows assurance that the service meets the established goals and good practices to avoid risk, regular back-up, the suitable selection of passwords and access privileges and contingency and data recovery plans in the event of disaster.

Trust is an essential factor in guaranteeing the success of this type of project, as it both ensures that the available tools are used and encourages the public to continue accepting and proactively using the said services. In this respect, it is important to emphasise the need to promote education and training and to underscore the exigencies related to security and the protection of personal data.



E-GOVERNMENT AND TELECOMMUNICATIONS

Likewise, the attitude of government employees also has a significant influence on the success of these projects, which involve changes in the services and administer information in a different manner.

Suitable public information regarding the scope and goals of e-government projects must also be envisaged in the design and implementation of these initiatives.

III. TELECOMMUNICATIONS

Telecommunications services constitute a specific area for personal data protection for two primary reasons: firstly, because the growing inter-operability and extension of these services have in themselves become a risk factor for data management in general, and private data in particular. Secondly, telecommunications processes require the determination and identification of the end-to-end points in the network making the communication, and such identification of data subjects may come to be considered as personal data.

The *Declaration of Cartagena de Indias*, drafted on the occasion of the *III Encuentro Iberoamericano de Protección de Datos* (Third Latin American Data Protection Conference) warned of the risks existing with respect to personal data processing and privacy in the telecommunications sector, and set out a list of such risks.

The Declaration presupposes the need to adapt guarantees that are capable of reaching a balance between personal data processing in the electronic communications services available to the public and the fundamental rights of the individual in the processing of personal data.

The demarcation of such guarantees must be founded on a basic premise of technological neutrality, which means that these guarantees will be effective regardless of the technologies used.

Customer traffic data processed in electronic communications networks when establishing connections and the transmission of data contain information regarding the private lives of data subjects and the legitimate interests of legal entities.

In particular, this data can be processed to draw up profiles of customers and users with a view to the commercial marketing of services, both in the definition of the services to be provided and in the planning of advertising campaigns. Likewise,



E-GOVERNMENT AND TELECOMMUNICATIONS

the data may be used to provide premium value services, which at times involve contractual obligation, without the consent of the user.

A similar situation exists with respect to the processing of location data that furnishes information about the physical location of a particular terminal in use.

The suitable balance in the processing of traffic and location data for purposes other than the provision of electronic services must include the prior, informed consent of customers to such processing setting out the specific purposes of the same. This requirement is particularly important with regards to the provision of premium value services.

The use of detailed invoices allows customers to verify the rates applied for the services, but also affects the privacy of the telecommunications services users. Therefore, alternative payment methods that guarantee privacy must be sought, and invoices that reflect only partial numbers called must be made available.

Advanced telephony services in digital networks make it possible to identify the line where the call originates and the line to which it connects. To protect the parties in this communication, the line from which the call is made should not be identified and calls from non-identified lines should have the option of refusal. These exclusions should not be operational when they affect public safety or emergency services.

Electronic communications directories are widely available and accessible to the public. The individual's right to privacy requires that data subjects be entitled to decide whether they want the data necessary for their identification published in such directories and if they consent to the use of the same for purposes other than as tools of reference.

Given the frequent use of directory data for advertising or promotional purposes, customers must be offered the option of including an indicator in such directories that excludes this type of use.

The evolution of electronic communications services and the information society is based, amongst other concepts, on the existence of effective security measures. Thus, service providers must adopt the necessary measures to safeguard security and inform customers and users free of charge of the particular risks involved and the actions they may undertake to protect the security of their communications.

Finally, an increasingly frequent phenomenon is the installation of devices in communications terminals that enable the storage and retrieval of data without the users' knowledge.

Users have the right to be informed of the installation of such devices and must be provided with a simple procedure to deactivate the same at no extra cost, except in those cases where they are essential to the provision of the services.

IV. SPAM

Technological evolution has greatly expanded the possibility of sending unsolicited bulk commercial communications through automatic diallers, faxes, e-mail messages and "sms".

Certain of these, such as the dispatch of unsolicited commercial e-mail messages ("spam") have reached disturbing proportions, given their massive scope.

"Spam" is a problem for individuals as, in addition to violating their privacy, it may lead to error or deception, or even represent outright fraud. It also implies spending time and money in the purchase of filtering or other types of programmes.

Moreover, it also involves considerable expense for companies, both directly (lower performance and productivity of employees and the investment of time and money in solving the problems) and indirectly (false positives, spreading of viruses). For Internet service providers (ISP) and e-mail service providers (ESP), it may entail the need to acquire a broader band and greater storage capacity.

At the same time, "spam" is a low-cost, highly profitable activity, particularly in cases involving fraud ("phishing" and others).

Finally, "spam" has reached global proportions and requires responses at an international level.

Therefore, "spam" can seriously undermine user trust, an essential factor in the progress of e-commerce in the whole of the information society.

A wide range of regulatory, technical and awareness measures, in addition to international cooperation, are all necessary to combat to this phenomenon.

Within the scope of regulations, the first issue is to establish a consensus on a uniform definition of the term “*spam*”, as the acceptance of different definitions will diminish the efficiency of the other measures undertaken and, in particular, will undermine international cooperation on this matter.

In this respect, the legality or illegality of “*spam*” must be established by the requirement for the informed consent of the user, either by prior consent (*opt in*) or at the very least, given the option to refuse reception (*opt out*).

Thus, it is important to consider “*spam*” illegal when it does not provide an effective procedure for refusing reception.

The regulations put into place must envisage penalties suited to the severity of the phenomenon, including blockage of the websites involved, and facilitate mechanisms for reporting *spam* and procedures to compensate the damage it causes. Therefore, specific authorities must be given the powers to apply such regulations and effective legal instruments must be drawn up to this effect. In addition, extra-legal alternative mechanisms for the resolution of these conflicts must also be encouraged.

The technical solutions addressed at putting an end to “*spam*” should include blocking of messages from servers identified as “*spam*” sources, user implementation of filtering programmes in their own terminals, and e-mail service providers implementation of the same in their own servers.

In this regard, it is particularly important to pay special attention to servers that operate in open mode and open “*proxy*”, that may be used to retransmit messages that are sent by the “*spammers*”. These servers must be obligated to adopt the security measures necessary to prevent any such retransmission.

However, filtering techniques may block important e-mails (false positives) or may not block “*spam*” (false negatives), causing problems that may lead to litigation. Thus, the conditions set out in customer contracts must be adapted so that the ISP/ESP’s and mobile service providers can offer their customers filtering options and include clauses that prohibit sending unsolicited e-mail.

It is essential to embark on awareness and educational measures so that the public clearly knows the risks posed by “*spam*” and the steps that must be taken to avoid it.



E-GOVERNMENT AND TELECOMMUNICATIONS

The efficient processing of cross-border complaints is also a vital part of making user protection possible, and hence, international cooperation is indispensable in this effort.

Such cooperation should encompass a twofold goal: one, to promote effective regulations in the countries in the region; and two, to encourage cooperation amongst the relevant authorities to guarantee that the regulations approved are suitably observed.

V. CONCLUSIONS

Finally, to fuel the development of e-government and personal data protection systems in telecommunications, we propose the creation of a forum in the website defined in the strategy document drawn up by the *RED* to furnish information on and the application of good management practises and to systematically identify relevant experiences that may be reproduced for subsequent diffusion, providing a global learning area.

Amongst others, this initiative should include a data bank of reproducible cases, e-government products (websites, on-line services, etc.), *bench marking* and a bibliography.

Huixquilucan (Mexico State), 4th November 2005