A methodological proposal for a National Survey of Data protection in E-Government in Mexico

Teresa M. G. Da Cunha Lopes

Available at: https://works.bepress.com/teresa_dacunhalopes/7/
A methodological proposal for a National Survey of Data protection in E-Government in Mexico

Teresa Maria Geraldes Da Cunha Lopes
tdacunhalopes@gmail.com

1 Ph.D. in Law; Master in “Sociedad de la Información y del Conocimiento”, UOC, Barcelona. Professor at “Facultad de Derecho y Ciencias Sociales”, UMSNH, Mexico
Summary:

The present research paper is an attempt to study the aspects related to e-government and data protection in Mexico, and at the same time, in view of the lack of empirical data presents a methodological proposal for the urgent implementation of a national survey. We focus in the protection of personal data used by public administrators to provide public services. Our primary objectives within this methodological proposal are the following:

1. To assess how prepared is Mexico, both at federal and state levels, to take full advantage of e-government and e-participation services
2. To assess how much Mexican administration, at federal, state and local levels, are currently benefitting from e-government and e-participation services and how it compares to other study cases
3. To assess data protection in Mexican administrations and comparative study cases from Latin America and EU as far as e-government and e-participation services are concerned

Introduction:

Advances in information and communication technologies are revolutionizing virtually every aspect of life and facilitating access to information in an exponential way. This is affecting governments and public administrations, which are exploring how to interact with citizens in order to provide better administrative services and facilitate participation.

On one hand, this calls for public administrations to reengineer their processes so as to benefit from ICT while, on the other, it means they have to facilitate citizen access to ICT and to introduce new automated processes requested by a citizenry aware of the potential ICT.

We are, therefore, facing the beginning of a revolution which will redefine the role of Administrations, brought about by elements such as databases which allow massive storage of information or networks which allow fast and secure communications. This revolution is contemplated in many governments IT strategic plans, as in the case of Mexico, but has not yet been fully realized in any country. Many issues are still to be debated and solved, including those related to existing regulations (or the lack of those regulations) for security and data protection.

---

2 This paper explores the effect of the lack of empirical data on managerial innovativeness in the three levels of government in Mexico on the adoption of e-government, and it examines the association between the adoption of e-government and data protection in Mexico. A comparative view can be found in M. Jae Moon & Donald F. Norris: Does managerial orientation matter? The adoption of reinventing government and e-government at the municipal level, *Information Systems Journal, Volume 15, Issue 1, Page 43-60, Jan 2005*

3 New technologies provide new channels of access to political information and participation in decision-making processes. This assumption is clearly important in the action plans and policies of International Organizations as stated in Francesco Amoretti: International Organizations ICTs Policies: E-Democracy and E-Government for Political Development, *Review of Policy Research, Volume 24, Issue 4, Page 331-344, Jul 2007*, but also at national level and transborder interactions.
Justification of the scope of the methodological research proposal:

There are many different challenges to be dealt with. To begin with, governments should be able to exploit all the potential of ICT, redefining and redesigning all their interaction processes with their citizens according to the available possibilities⁴. Yet, only a systematic and far reaching study of all the implications generated by the use of ICT in public administrations can provide a coherent view of the range of e-government processes and e-services participation, and of their potential, without attacking or degrading the constitutional rights of the citizens involved.

We think that the establishment of electronic management systems constitutes a decisive element in increasing the quality of the relations between public administrations and citizens⁵. Such systems raise the level of efficiency in public services, increase the degree of the interactivity with the citizenry and may raise the quality of services and their acceptance by the addressees⁶. As a matter of fact, the Internet and the e-government platforms provide powerful tools for reinventing local governments. They encourage transformation from the traditional bureaucratic paradigm, which emphasizes standardization, departmentalization, and operational cost-efficiency.

However, electronic management systems imply the collecting and processing of personal data. For this reason, it is absolutely necessary to detect potential problems relating to data protection on the Internet (including the ones connected to international data transfer). Therefore we must assess the risks involved and study the appropriate solutions, not only within technical parameters but with legal instruments and the correspondent judiciary implementation protocols. For example: While the Internet has popularized the notion of “beyond borders”⁷, the reality is that even more items of personal data are “crossing borders.” From formal applications for visas and work permits, to business transactions, to informal voice and data communications, personal information makes its way from one country to another. Some of this data flow occurs with the knowledge and possibly the consent of individuals, but much of it is in the backdrop of administrative noise to which most people do not attend. These largely invisible flows of personal information contribute to an individual’s record of personal transactions with a range of organizations (including business, health care and government, as well as becoming an item in the exchanges of record systems between organizations.

---


⁵ Despite the reservation we stated in note 3, electronic government, or e-government, increases the convenience and accessibility of government services and information to citizens. See: Christopher G. Reddick and Howard Frank : E-Government And Its Influence On Managerial Effectiveness: A Survey Of Florida And Texas City Managers , Financial Accountability & Management, Volume 23, Issue 1, Page 1-26, Feb 2007


⁷ See: Kahin & Nesson, 1997
Privacy Rights and Data Protection: legal concepts and globalized iurisprudentia

Before developing this idea any further, I would like to dwell at some length on the notions of “privacy”\(^8\) and of “what privacy is for.”

The notion of privacy can be approached in two different contexts\(^9\), to which we will refer as the context of civil society and the context of political organization of power. In the context of civil society, the term privacy is used to refer to those aspects of one’s self that each individual withdraws from general knowledge and keeps apart from society; by opposition, publicity can be identified with the areas of one’s self that are exposed to other individuals in such a manner and to such an extent that they can be considered part of a space occupied by all. In the context of political organization of power, on the other hand, the term publicity refers to political power, whereas privacy refers to civil society to the extent that it is distinct from the former. Here the distinction between privacy and publicity goes along the line that modern states have drawn between the public person or sovereign and the private person or citizen. In the political context privacy is opposed to and claimed against the political power; in the civil context it is primarily opposed to and claimed against society. We say primarily because, although civil privacy is conceived as areas of oneself kept away from society, political power is by no means innocuous with respect to it.

It can threaten the areas that individuals intend to keep apart from society and can do so to a much greater extent than society itself.

This is why some areas of civil privacy, such as the inviolability of one’s premises or of the secrecy of one’s telecommunications, are often protected also against political power by fundamental rights.

The use of the term privacy is thus difficult to contain of the two contexts in which it can be used, our interest lies exclusively in what we called the civil one. We will therefore overlook the fact that privacy also stands for civil society and will depart from a definition of privacy that conceives it as an area of one’s self that one wishes to withdraw from the presence and knowledge of others. In brief, we conceive privacy as one’s seclusion and one’s secrecy—or more precisely as control over one’s seclusion and secrecy. This is also the most common use of the term privacy. It is, above all, supported by the definitions of privacy provided by dictionaries, which rest both on the notion of seclusion, or withdrawal from society, and on the notion of secrecy, or concealment from the public eye.

In legal circles too there seems to be wide agreement on the inclusion of one’s seclusion and secrecy within this concept, very much in contrast with the controversy that surrounds the inclusion of some other areas. For the term “privacy” and the corresponding

---


10 A good example is Richard A. Posner, who points to the distinction between “privacy” and “the purposes for which people want privacy” and yet draws no conclusions from it.
expression “right to privacy”11 are used by courts and commentators in a variety of ways, to refer not only to one’s seclusion and one’s secrecy, but also to areas as diverse as one’s reputation, one’s name and likeness or one’s autonomy to take intimate decisions (the “right to be left alone” in Griswold vs. Connecticut)—or rather to refer to one’s control over each one of these areas. The question of which areas belong to the concept of privacy is the object of permanent controversy in specialized literature.

More interesting and more relevant for us is how one’s autonomy to take intimate decisions relates to the concept of privacy as control over one’s seclusion and secrecy that we have adopted. Consider, in particular, that in the case of one’s seclusion and secrecy privacy denotes an idea of shelter or of freedom from intrusion, whilst in the case of the area of one’s autonomy to take intimate decisions privacy is rather conceived as freedom to act or to carry out certain activities beyond the intrusive eyes of the state, notably under the shelter of privacy. In other words, if one’s secrecy and seclusion is equated with privacy and the shelter it provides, one’s autonomy to take intimate decisions is not an instance of privacy itself, but is rather an instance of what we want privacy for.

The above considerations on the notion of “privacy” have thus led us to the notion of “what privacy is for.” Privacy has been identified with control over one’s areas of seclusion and secrecy; accordingly, the right to privacy amounts to the right to exercise that control, primarily against society but also and more importantly against the state. What privacy is wanted for is one’s autonomy to take intimate decisions or, more broadly, one’s autonomy to take and carry out decisions in private.

If individuals want to keep control over their areas of seclusion and secrecy it is in order that they can exercise their autonomy free from the intrusive eyes of both the public power and society. As we stated before, in the case of Mexico, as in the EU, Privacy rights are defined as a fundamental human right and have constitutional protection.

Yet, as we attempt to give a definition of “privacy rights” and its legal meaning, another problem arises that makes this proposal for a national survey and the construction of national indexes for Data Protection in E-government in Mexico an urgent task. We are referring to the recent EU Data privacy regulation and its transnational jurisdictional effects.

EU data privacy regulation poses multiple threats to Mexico government based data and to Mexico companies, and to the flow of data between the two countries, and also, as a non-intended consequence, to the flow of data between Mexico and the United States12.

The EU, upon a proposal of the Commission approved by a qualified majority vote of Member States, may ban all data transfers to countries which fail to ensure adequate data privacy protection (Directive13, Articles 25, 31). Even if, as appears likely for political


13 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. 23.11.95 L281/1
reasons, the Commission refrains from finding that Mexico (with whom it has signed a Free Trade Agreement during President Ernesto Zedillo mandate), as a whole, inadequately ensures data privacy protection, it can limit its determination to certain economic sectors, types of information or operations. Member State authorities can also independently fine individual companies and enjoin them from transferring data, including to their mexican affiliates, and even imprison company officials.

The Directive is now in force and has taken a life of its own. Private parties and Member State authorities can use it before courts and administrative bodies in ways that the original draftsmen did not predict. The Mexico-EU dispute over the adequacy of Mexico data privacy protection affects Mexico privacy policies (at the three levels of government) and practices because the EU exercises market power. The EU is one of Mexico’s largest trading partner and the origin of most Mexico foreign investment (also, as stated above, we must take into account that this EU Directive also affects the data transfer between Mexico and the USA, as a consequence of the transnational jurisdiction of the Directive).

A potential restriction on transatlantic data flows matters and it’s a powerful argument to the strict implementation of the existing Mexico federal regulation on data protection at federal, state and local level, to the expanding of data protection to the private sector and to the legislative reforms that, at present, are being discussed by the Mexican Senate.

EU collective market power provides EU officials with considerable bargaining leverage over data privacy issues. Were a country (or region) that attracted little mexican trade and investment to restrict data transfers to Mexico, a ban would pose little harm to overall Mexico political and commercial interests. More importantly, that country’s exports would be disproportionately vulnerable to access restrictions to the much larger EU market. Mexico retaliation against the EU, on the other hand, could give rise to counter-retaliation seriously harming Mexico political and commercial interests.

The EU Member States have not simply ‘lost’ sovereignty in working through centralized EU authorities. They have reallocated it in a manner which effectively enhances their negotiating authority (and in that way their autonomy) vis-à-vis other states sovereignty. Mexico increasingly negotiates with the EU as an independent political institution apart from its 27 Member States. Yet, the extra-jurisdictional effects of EU regulatory dictates can be constrained, and Mexico national autonomy preserved, by supranational trade rules, for example by challenging any ban imposed by the EU before the Dispute Settlement Body of the World Trade Organization.

There are arguably some protectionist motives behind the Directive. Since personal data is a non-standardize product, were Mexico to challenge any EU data transfer restrictions, the claim would most likely be assessed under the General Agreement on Trade in Services (GATS). WTO members’ obligations are more limited under GATS than

---


15 Under GATS article XIV, WTO members may adopt and enforce measures that restrict trade in services which: ‘Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, . . . [are] necessary to secure compliance with laws or regulations not inconsistent with the provisions of this Agreement, including those relating to: . . . (ii) the protection of the privacy of individuals in relation to the processing dissemination of personal data and the protection of confidentiality of individual records and accounts’
under the General Agreement on Tariffs and Trade (GATT) 1994. Most GATS obligations only apply if the service operation in question is specifically included in a schedule of market access commitments, which involve hundreds of pages of detailed commitments and qualifications. Only when a data transfer is so covered is the EU obliged to treat Mexico services and service providers as favorably as EU services and service providers (GATS Article XVII), and to apply its domestic regulation in a ‘reasonable’ manner (GATS Article VI). In addition, were the EU to ban data transfers only to Mexico, but not to other WTO members with inadequate data privacy protection, the EU would violate the GATS most-favored nations’ clause (Article II).

Even where a data transfer is covered by a specific EU commitment, Mexico would likely not prevail in an action before the WTO Dispute Settlement Body for three primary reasons. First, on its face, the Directive applies equally to EU-owned companies and registered, and foreign-owned and registered, companies and thus should not violate the GATS national treatment or most-favored nation clauses (or the Free Trade Agreement in place).

One of the four major goals of the EU Agenda is ‘to create a New Transatlantic Marketplace, which will expand trade and investment opportunities and multiply jobs on both sides of the Atlantic’ and contribute ‘to the expansion of world trade and closer economic relations.’

Second, the EU has a legitimate public policy objective—to protect the privacy of EU residents who are the subjects of data transferred to Mexico. The GATS general exception clause, Article XIV, explicitly authorizes WTO members to restrict commerce in order to protect ‘the privacy of individuals,’ significantly bolstering the EU’s defense. Given that the privacy interests of EU residents are directly at stake, it is unlikely that a WTO panel would find non-discriminatory restrictions applied under the Directive to be ‘unreasonable.’

Third, the WTO Appellate Body, under close media scrutiny, would prefer to refrain from engaging in a close balancing of trade and privacy interests, and rather review the process by which the EU takes account of foreign privacy protections. WTO rules are often criticized for limiting the ability of countries to enact socially oriented legislation. They are primarily ‘negative’ rules, obligating states, among other matters, not to restrict imports on account of non-product-related foreign production methods, such as ‘unfair’ environmental or labor practices that result in foreign environmental harm or foreign labor repression. Paradoxically, in the case of data privacy, rather than protecting Mexico from coercion to raise Mexican privacy standards, WTO rules shield the EU from a countervailing retaliatory threat. Were Mexico to retaliate against the EU for harming Mexico commercial interests and coercion over its federal data protection regulatory reform, it would itself violate WTO rules and be subject to an EU complaint. WTO rules thereby reinforce pressure on the US to negotiate with the EU a set of ‘positive,’ more stringent, data privacy requirements. WTO rules thereby contribute to a trading up of Mexico standards.

Data privacy regulation in Europe informs not only the tenor and context of debates in Mexico, it shapes interest groups’ appreciation of their options, adding pressure to national legislation reform. In this context we think that Mexico needs to build analysis tools that could provide the executive and legislative branches with accurate information.

---
about Data Protection in E-Government at federal, state and local levels in Mexico. Thus our methological proposal.

A methodological proposal for a National Survey of Data protection in E-Government in Mexico

The methodology approach we propose for a National Survey of Data Protection in E-Government in Mexico stems from the study by the United Nations in their e-Government Readiness Reports, conveniently modified to address the Mexican context, and is complemented by our aim of considering data protection issues. Therefore, we shall assess e-government, e-participation and data protection at the diverse levels of Mexican Public administration. Because of data availability we shall give different status to some of Mexican Federal Sates (e.g. Colima). A major difficulty arises in the determination of the concepts Data Protection and Privacy and the appropriate indexes to measure their level in E-Government: some countries, notably the United States and to a somewhat lesser extent Canada and France, defined their protection in terms of privacy, while other countries, including Mexico and most of the European countries (as Spain and Portugal), characterized theirs as data protection. Additionally, some countries adopted omnibus legislation requiring public and private organizations to comply while others passed sectorial legislation establishing different standards for public and private organizations as well as within the private sector.

Or, as in the case of Mexico, the federal regulation only requires the three levels of the public administration to comply with Data protection measures but leaves a legislative vacuum in all matters concerning the private sector and the interaction of citizens with business databases and general private services.

With the passage of national privacy or data protection legislation, national variations generated regional and international conflict. An often-quoted statement of France’s Magistrate of Justice at an Organization for Economic Cooperation and Development (OECD) symposium in 1977 captures this conflict: “Information is power,

---

17 Part of the remit of public sector management includes planning and reflecting on capital expenditure on new technology. With this in mind, the role that information systems play in supporting improvements in e-government service delivery to the society will also be a part of the final project implementation. For this purpose we use: Lemuria Carter & France Bélanger: The utilization of e-government services: citizen trust, innovation and acceptance factors, Information Systems Journal, Volume 15, Issue 1, Page 5-25, Jan 2005

18 Privacy and data protection are being constructed almost simultaneously on the national and transnational levels. This proposal thus provides also a rich opportunity to explore the interactions between international structures and national agents in development of a norm that is central both to human rights and also to global trade. The interdependence generated by global trade and the transnational convergence of values provoked by global consumerism and global concern with human rights may create incentives for the development of more collective or shared identities regarding privacy and data protection. See: Zahir Irani, Peter E.D. Love, Tony Elliman, Steve Jones & Marinos Themistocleous: Evaluating e-government: learning from the experiences of two UK local authorities. Information Systems Journal, Volume 15, Issue 1, Page 61-82, Jan 2005

and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows”.

This quote emphasizes the marketable, technological, and national sovereignty components of the debate about the exchanges of personally identifiable information across different national jurisdictions. But, also, other components of the problem have received attention, including the human rights concern with personal privacy and concern with the free flow of information. Each component emphasizes a distinct aspect of the problem, generates particular questions in policy deliberations, and elicits different configurations of the indexes analysis.

Given diverse cultural traditions and varying involvements in international trade, countries define the problem of data protection in E-Government and specifically the problem of transborder data flows somewhat differently. For example, the United States generally stresses the free flow of information, often citing the First Amendment in support, and the importance of a free market. In contrast, we argue that the Mexican perspective, which interprets privacy and data protection policies as most of the UE countries is rooted in the traditional government control process typical of civil law societies and avoid market solutions to consumer complaints, and the value of information to a market economy.

In Mexico, privacy issues are driven by constitutional theory and not by consumerism and free trade as is the case in the USA. Following the European and some other countries Latin American countries, privacy and data protection policies protect fundamental rights of citizens. They reflect a tradition of more government control over the economy and information flows, and the belief that governments have a duty to protect the privacy of their citizens. They emphasize not only their human rights traditions, including privacy, but also, in light of the power of American transnational companies, national sovereignty. With American and European variations in national privacy or data protection laws views about the role of government, and orientations to free trade, conflict over transborder data flows would not be surprising as far as Mexico (a “bridge-country”) is concerned.

These national differences appear also, to some extent, in public attitudes about privacy and information flows, especially about commercial transactions, but there are also some commonalities in national attitudes20.

---

20 For comparative purposes: in Spring 1999, IBM commissioned a survey in the United States, Germany, and the United Kingdom regarding consumers’ attitudes about privacy and consumer marketing. Telephone interviews, averaging 20 minutes in length, were conducted with a national cross section of 1,006 adults in the United States, 1,002 in the United Kingdom, and 1,000 in Germany (IBM Global Services, 1999, p. 8). The report provides percentages but no statistical tests. The majority of consumers in all three countries were not very interested in receiving marketing material: Consumers in the United States (48%) were more interested in receiving marketing material than consumers in Germany (32%) or the United Kingdom (29%; IBM Global Services, 1999, p. 11). Although these results reinforce the perception of a more consumer-oriented culture in the United States, they do not mean that Americans are necessarily less concerned about the privacy issues related to marketing. Indeed, virtually identical percentages of respondents in the United States and Germany believe that they have lost control over both how information is collected and how it is used by companies (United States 80% and Germany 79%) and that it is impossible to protect privacy in the computer age (United States 71% and Germany 70%). Respondents in the United Kingdom express a slightly less pessimistic attitude (IBM Global Services, 1999, Exhibit ES-3, p. 22). A higher percentage in the United States (64%) trusts that businesses are handling personal information in a proper and confidential manner than in the United Kingdom (58%) or Germany (54%; IBM Global Services, 1999, Exhibit ES-3, p. 22). It is unclear whether these national differences stem from views about the effectiveness of laws or views about trust in business. Interestingly, the cross-national responses regarding the reasonableness of protection offered by existing laws do not parallel the responses regarding trust in business practices.
By comparison, Mexico which has adopted a range of privacy or data protection federal policies has yet to produce a reliable national survey of Data Protection in E-Government. Thus the construction of this methodological proposal.

In the construction of the evaluation of the indexes we consider the following fields:

1. e-Government Assessment
2. e-Government Readiness Index
3. Telecommunications Infrastructure Index
4. Human Capital Index
5. Web measure Index
6. e-Participation Index
7. Data Protection Index

These fields determined the following Working Index proposal:

I. Introduction
   1.1 Information technologies in the new society
   1.2 The Millennium Project and the Tunes Conference
   1.3 The CLAD charter
   1.4 Existing challenges
   1.5 Objectives

More respondents in the United Kingdom (63%) find their legal and organizational practices reasonable than in the United States (59%) or Germany (55%), which reports the lowest percentage of respondents agreeing (IBM Global Services, 1999, Exhibit ES-3, p. 22). Survey results did indicate a difference in some behaviors among respondents in the three countries. For example, Americans (78%) “refused to give information” compared to the English (58%) or Germans (52%; IBM Global Services, Exhibit ES-4, p. 23). The basis for this difference is unclear. The larger percentage in the United States could be attributed to more distrust of business, but this interpretation would contradict the level of confidence in business handling of personal information. Instead, it may be accounted for by more, and possibly more intrusive, requests for information by U.S. businesses and the more developed direct marketing presence in the United States. There were also differences in the “comfort level” that respondents in all three countries had with the “way government is handling protection of consumer privacy.” Responses to the IBM survey demonstrate that there is cross-national agreement about the loss of consumer privacy. The results indicate there is room for the social construction of common governmental and organizational practices to protect consumer privacy. I would argue that businesses’ collection of personal information is a universal phenomenon and, with global trade and global companies, there will be pressures for more similarities among national business practices for the handling of personal information. Businesses, across nations, prefer fewer restrictions on the handling of personal information.

21 The challenge towards e-democracy, through the electronic transformation of political systems, has become increasingly evident within developed economies. It is regarded as an approach for increased and better quality citizen participation yet it contains also the tools for the implementation of totalitarian systems. See: Harald Mahrer & Robert Krimmer ; Towards the enhancement of e-democracy: identifying the notion of the ‘middleman paradox’ Information Systems Journal, Volume 15, Issue 1, Page 27–42, Jan 2005 and Villalón Alejo, Lucia & Teresa Da Cunha Lopes: La Democracia Electrónica en la Sociedad de la Información, in Da Cunha Lopes , Teresa; Luviano G., Rafael; Revuelta V., benjamin &Sánchez B., Roberto : Globalización, Derechos Humanos y Sociedad de la Información, pp. 101-130

22 On the question of objectives the reader must remember that this paper presents a commitment transformation framework for analysing the “change in actors’ commitment during the transition from escalation to de-escalation in information technology projects in E-government. See: Caroline J. Tolbert, Karen Mossberger& Ramona McNeal : Institutions, Policy Innovation, and E-Government in the American States , Public Administration Review, Volume 68, Issue 3, Page S49-S63, May 2008
1.6 Methodology

II. E-Government and e-Participation assessment in Mexico and comparative Study Cases

2.1 Mexico e-government and e-participation in Mexico
2.1.1 e-Government assessment readiness
2.1.2 Telecommunications Infrastructure
2.1.3 Human Capital
2.1.4 National Strategic Plans for the Information Society
2.1.5 E-Participation

2.2 Latin America Comparative case Studies Assessment: Chile and Brazil

2.3 Europe Comparative Case Study Assessment (EU)

III. Data Protection in e-Government

3.1 Mexico
3.1.1 General Regulation on Data Protection
3.1.2 Special Regulations
3.1.3 E-Government and Electronic Communications Regulation
3.1.4 Duty of Information
3.1.5 Data subject Consent
3.1.6 Claims
3.1.7 Control Authority
3.1.8 Security measures
3.1.9 Data Subject Rights

3.2 Latin America Comparative Study Cases Assessment: Chile and Brazil

3.3 Europe Comparative Study Case Assessment (EU)

IV. Conclusions

V. Indexes

---


24 Mexican grassroots governments have rushed to join the e-government revolution. Although there is a growing body of e-government literature, little of it is empirical. Using data from two nationwide surveys and from comparative UE databases, will allow us to conduct a longitudinal examination of local governments and to analyse its comparative level of performance. We intensively used as a comparative methodological analysis: Caroline J. Tolbert & Karen Mossberger: The Effects of e-Government on Trust and Confidence in Government, Public Administration Review, Volume 66, Issue 3, Page 354-369, May 2006

25 Trust in government has been declining for more than three decades now. e-government has been proposed as a way to increase citizen trust in government and improve citizen evaluations of government generally yet due to the non existent policies of data protection there is a perpetual mistrust of the handling of citizens personal data by mexican government agencies in the three levels of public administration. See: Alfred Tat-Kei Ho: Reinventing Local Governments and the E-Government Initiative, Public Administration Review, Volume 62, Issue 4, Page 434-444, Jul 2002
5.1 e-Government Readiness Index
5.2 Telecommunications Infrastructure Index
5.3 Human Capital Index
5.4 Web Measure Index
5.5 E-Participation Index
5.6 Data Protection Index

BIBLIOGRAPHY


Vargas, Jorge A. :Privacy rights under Mexican law: emergence and legal configuration of a panoply of new rights." Houston Journal of International Law 27.1 (Fall