Analyzing the Best Practices of Information Security and Protection of Sensitive Data in the Context of e-Government in Colombia and Chile

Gastón Concha
Universidad Santo Tomás
Ejército 146,
Santiago, Chile
+56 2 2 9384611
gconcha@santotomas.cl

Paula Suárez
Universidad Externado de Colombia
Carrera 64 # 24-47 apartment 503,
Bogota, Colombia
+57 313 8306908
paucasuarez@gmail.com

ABSTRACT
This article is the result of a research project on information security and protection of sensitive data in Colombia and Chile, since information security is a fundamental issue for the protection of individuals' and companies' data, especially when said information is contained in an unregulated environment such as the Internet, and when countries under development such as Colombia and Chile are close to implementing electronic government. The regulations and the current state of the protection of sensitive data in both countries will be analyzed in this paper, using as a reference the good data protection practices defined by the European Union and the United States. Additionally, the paper reviews information security and data protection within the Ministry of Information Technology and Communication analyzing the likelihood of threats to the integrity, confidentiality and availability of information in the notification process to determine whether Colombia is prepared to guarantee flexible on-line procedures online as well as secure information and legal certainty to citizens.

Categories and Subject Descriptors
K.4. **[Computers and Society]:** Public Policy Issues

General Terms
Documentation

Keywords
Information Security; e-Government; Right to Privacy; Sensitive Data

1. INTRODUCTION
E-government refers to "*the availability of information from government agencies and some public services throughout Internet, it means that officials and politicians use information technology and communication (ICT) for the restructuring of state agencies, operations and relationships between agencies and NGOs*." Such availability of information has begun to generate huge discussions related to privacy rights, privacy, and confidentiality, due to the fact that data retention and transmission of information from one entity to another may affect the legal security of citizens, which in turn related to personal data privacy.

However, there are many cases exemplifying the right to information and implementation of online government and open data catalogs currently being promoted by versus the basic principles of information security, such as data confidentiality, availability and integrity, in addition to the right to protect personal data.

Furthermore, the increasing presence of virtualization strategies or cloud computing for managing government IT assets (G-Cloud) sparks other challenges regarding data security and protection. In this regard, various government agencies have established guidelines for incorporating insurance Cloud Computing models, for example, the Information Commissioners' Officer (ICO) in the UK provides a guide on the use of cloud computing within the framework of the Data Protection Act 1998 (DPA)[1], while the Spanish Agency for Data Protection also has a similar guide with a special chapter related to the government [1]. Finally, it is noteworthy to mention the report prepared by The European Network and Information Security Agency (ENISA), entitled "Security & Resilience in Governmental Clouds" in 2011 as another guide for the public sector to define legal, operational information security and resiliency aspects, constituting actual support to European Union Member States in defining their cloud strategies in relation to these issues.

2. ANALYSING THE CONCEPT OF THE RIGHT TO PRIVACY OR COMPUTING FREEDOM

Freedom computing, *"a concept derived from the right to privacy, and that ensures that the identity of individuals will not be invaded or used for illicit purposes, through new technologies either by the State or by individuals* [1]". The right to privacy is divided into: (i) physical intimacy, (ii) personal safety, (iii) personal freedom; and (iv) privacy informative. For this case, we are only interested in defining the privacy informative, which

ICEGOV2013, October 22-25, 2013, Seoul, Korea

[1]http://www.ico.org.uk/for_organisations/data_protection/the_guide

refers to *"the autonomy of individuals to communicate or not, their personal data*[2]*."*

2.2. Definition of Privacy

Privacy is the right of individuals to protect their own information. The protection of privacy in the use of information and communication technologies is defined by five principles (Table 1).

Table 1: Five privacy protection principles

Notification principle	Defines the right of the individual to be informed or notified on the storage, use and disclosure of his or her personal data.
Choice principle	It implies that people have the right to choose autonomously whether to allow the use of their personal information.
Access principle	This relates to the right to informational privacy, since people, and in this case citizens, have the right to access databases and websites where personal data is stored.
Safety principle	Refers to the access control mechanisms that must be employed by entities that collect sensitive information such as personal data
Regulatory principle	To ensure data protection regulation is a form of control and that companies or public agencies are subject to penalties if they store, use and disseminate information of individuals without permission and filters.

2.3. Why is it important to protect personal data in an open government?

The protection of personal data is necessary in the context of an open government for two reasons; firstly, because the right to privacy is a fundamental right, therefore the State must ensure the legal security of individuals; secondly, the right to privacy prevails over the right to information.

2.3.1. The right to privacy as a fundamental right and principle of rule of law: Both Colombia and Chile under the concept of social rule of law, founded on the principle of human dignity, must protect the honor and rights of individuals, as well as their privacy and intimacy, as recognized in the constitutions of both countries and in Article 12 of the Universal Declaration of Human Rights, stating that "no one will be subjected to interference in its privacy."

2.3.2. The right to privacy takes precedence over the right to information: Intimacy as a personality trait takes precedence over the right to information. As argued by Edgar Escobar and Luz Marulanda, when there is conflict between the right to information and the right to intimacy or privacy, the first takes precedence over the second, because it has a direct relationship with the principle of human dignity, which is an inherent human attribute that can only be limited in the event of general interest [1].

3. LEGISLATION AND CURRENT STATUS OF SENSITIVE DATA PROTECTION IN CHILE AND COLOMBIA

3.1. Privacy Legislation in Chile

Law No. 19,628: There is a category of personal data that receives the greatest level of protection and the law defines sensitive data as data referring to "physical or moral persons or facts or circumstances of his/her private life or privacy, such as personal habits, race, ideologies and political opinions, religious beliefs or convictions, states of physical or mental health and sex life." It seeks to regulate data stored and organized in records or databases held by both public agencies and individuals, to thereby ensure that no data are regularly found loose or left out of these electronic devices. However, protection does not preclude recognizing that disseminating such data is also a social necessity. In the end, it is all about leveraging the social benefits afforded by new information technologies in a way that respects the rights of individuals [7].

In Chile the right to privacy, enshrined in Article 19, Paragraph 4 of the Constitution, is defined as the right to "respect and protect the privacy and honor of the individual and his/her family."

The law prohibits the processing of sensitive data unless authorized by law, consent or there is data necessary to determine or grant health benefits corresponding to their holders (Art. 10).

3.2. Legal Framework for the Protection of Personal Data in Colombia

Statutory Law No. 1581 of 2012 concerning the right to data protection, it is a constitutional right of individuals to know, update and correct personal information contained in databases held by public and private entities. This law does not regulate: (i) databases for personal or household use; (ii) the data or files relating to national security; (iii) databases for monitoring and controlling money laundering; (iv) databases intended for intelligence and counterintelligence; (v) news and reporting databases; and (vi) databases regulated under Law1266.

Act 1266 of 2008 regulates personal information contained in credit, finance, trade and services databases. However, the law will be applied in accordance with the principles of confidentiality or reservations of certain data, and it applies to databases for statistics, research or punishment of crimes or to ensure public order.

4. RISKS AND OPPORTUNITIES OF OPEN DATA IN THE CONTEXT OF OPEN GOVERNMENT.

It is interesting to note that the statement of commitment by governments to the Open Government Partnership[3] to which both Chile and Colombia are parties, does not explicitly or implicitly mention the possibility that open data principles may conflict with the aforementioned principles of privacy and security of information. We therefore appreciate that at least the new digital strategy of the U.S. government in the document entitled: "Building a 21st Century Platform to Better Serve the American People[4]," states Security and Privacy as one of the four principles governing the new strategy. Therein is explicit mention of the need for greater data openness by adopting new technologies, has the potential to make data more vulnerable to malicious use and possibly violation of privacy. It is therefore necessary to strike a proper balance between protecting sensitive data and the need for

[2] Ibidem

[3] http://www.opengovpartnership.org/open-government-declaration

[4] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html#secure-new-technologies

government open data. In this sense technology can play a leading role.

5. GAPS IN CURRENT CHILEAN AND COLOMBIAN LEGISLATION

Table 2: Gaps in Current Chilean and Colombian Legislation

Gaps in Colombian Legislation	**Gaps in Act 1268.** It contains a limitation related to
	Operator abilities The operator can charge people for accessing databases, and these databases may market data with third parties without requesting prior authorization from the client The operator is released from liability if he posts incorrect information since he may show his "innocence" by proving that he acted in a professional manner or by proving that a third party was at fault. The operators have the ability to determine whether the other country granted access to such databases, ensures the best data protection conditions. **Preposterous fines for violating data protection** Fines imposed on operators for violating data protection law in finance and credit are preposterous, as these will be imposed according to the extent of the damage and the profit obtained by the offender by publishing said information.
	Gaps in Law 1581, 2012
	Several flaws related to the specific regulation Act 1581 has several flaws related to the specific regulation for personal data such as: (i) health-related information, (ii) telecommunications data, (iv) databases for advertising purposes, and (v) data transferred internationally. **Preposterous fines for violating data protection** Similar to Law 1268, statutory law 1581 makes the same mistake regarding the calculation of fines applicable to those who do not comply with the rule.
Gaps in Chilean legislation	**Absence of an effective control body** According to Rajevic, there are shortcomings in the Chilean legislation on data protection, such as the absence of an effective control body. As a result, Chilean legislation does not fully comply with OECD 5 guidelines and standards under Directive 95/46/CE6 EU, declaring Chile a safe country for the flow of data from its member states. (Both Argentina and Uruguay already met this requirement in 2006 and 2010, respectively) **Sanctions** Article 22 instructs the Civil Registry and Identification Office to keep track of public agencies' personal data banks, regulated under DS N° 779/2000, issued by the Ministry of Justice. However, there are not any sanctions for breaching this responsibility.

6. INFORMATION SECURITY AND PROTECTING SENSITIVE DATA

6.1. Definition and Basic Principles of Information Security.

Information security refers to preventive or reactive mechanisms to protect information within a public or private sector organization. Among these principles are: (i) availability, which guarantees access to information upon prior authorization by the person and in a controlled manner; (ii) confidentiality, which refers to the non-disclosure of information without permission; and (iii) integrity, which is necessary to ensure there are no unauthorized changes to the information

6.2. Relation between Information Security, Protecting Sensitive Data and Open Government

One of the principles governing the right to privacy is security. However, security of information is not only a issue of who has access to the data. In addition, information security controls and manages: (i) administration of information assets; (ii) roles and responsibilities of officials before and after use, with respect to accessing and managing information; (iii) physical and environmental security of the data; (iv) equipment safety; (v) communications and operations management; (vi) access control; and (vii) acquisition and maintenance of information systems. Therefore, the security of personal and organizational data does not only entail access control. It is essential for both public and private institutions to implement security measures for sensitive data, with respect to biometric controls, monitoring staff in policy formulation and implementation of information security, as well as guaranteeing citizens the freedom of information. The State must ensure that the information handled by pubic entities complies with the principles of information security, because should the right to intimacy be violated, discriminatory practices would be legitimatized and thus human dignity as well.

6.3. The Colombian Case: Data protection and Information Security

The Colombian Ministry of Information and Communication Technologies (MINTIC) is responsible for "defining the policy and practices pertaining to administrating, planning and managing radio, postal and related services. To this end it needs to notify stakeholders, dealers, network and service suppliers, and postal operators administrative act rulings (resolutions, contracts and orders) issued by the Ministry of ICT."

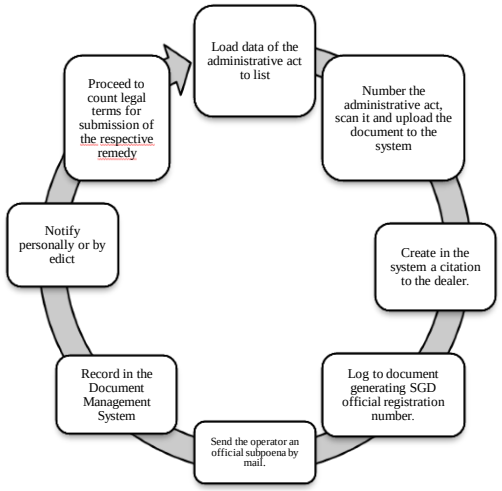

Figure 1: Notification Process MINTIC

[5] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", de 23/09/1980.(http://www.agpd.es)

[6] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

As part of a class exercise on Internal Audit of Information Security, officials from the Office of IT, Ministry of Information Technologies and Communications of Colombia, showed clear flaws in the security system and in the process of notifications issued by that entity, since as shown in Table 3, the availability, confidentiality and integrity of information assets, ranked people, technologies and processes, demonstrating a high risk that the data used in the notification process are vulnerable to failures in safety systems of information, taking into account that the probability of potential threats and vulnerabilities are divided into the following variables ,where one (1), means that vulnerabilities or threats to information are likely to occur and five (5) indicates that it is likely that threats or vulnerabilities will arise and threaten the confidentiality, integrity and availability of assets. The average of the criticality index is 3.96.

Table 3: Evaluation Matrix: Information Security of the Assets Involved in the Notification Process [8]

Information assets		Confidentiality	Integrity	Availability	Criticality
People	Location				
Concessionaire	External Location	3	3	3	3
Applicant	Functional Area	4	4	5	4.3
Notified	Officer functional area	5	4	5	4.7
PACO Coordinator	PACO: first floor	5	5	5	5
Numerator	Third floor	5	5	5	5
Technology	Location				
Computers	Database	5	5	5	5
Network	Infrastructure	4	5	5	4.7
Information Systems	PACO [7] functional areas	4	5	5	4.7
Numerator	Third floor general secretary	2	3	3	2.7
e-mail	TI area	5	4	4	4.3
Scanner	www.siust.gov.co	4	3	4	3.7
Processes	Location				
Frequency Allocation	Mission Area	5	4	4	4.3
Billing and Accounts	Support Area	3	4	4	3.7
Postal Services Enabling	Mission Area	5	4	4	4.3

Although the notification process is defined by the civil procedure code as "make known and public to stakeholders and an authorized third party the judge's decision in order to allow the parties to abide by or contest the ruling," flaws in information security do not only affect the effectiveness of the process but also free competition and corporate espionage, since communications made by the Ministry can be easily "heard" and thus distort processes such as auctions or bids.

[7] PACO: Point of Attention to Citizens and Operator

7. CONCLUSIONS

It is possible to guarantee citizens the right to privacy or confidentiality of information in an open government. In Colombia and Chile, the law protects the fundamental right to privacy and an individual's reputation. However, information security in public agencies and the creation of an oversight body to monitor the implementation of laws relating to data protection are still in the implementation stage, thereby creating risks for citizens, as they are exposed to a situation in which their information may be accessed without authorization. Laws, such as EU legislation, reveal that it is possible to regulate the access, transfer and storage of sensitive data of individuals, and that this is not contrary to electronic governments and the evolution of these so-called open governments.

Outsourcing data management by public entities in Colombia is another area warranting study in terms of data protection in the context of electronic governments. Shortcomings in information security management systems in public entities in Colombia also show that they are not yet able to collect and manage citizen data responsibly. Additionally, even the issue of protecting the rights to information and privacy is ambiguous, since case law has not established which of the two rights takes precedence should they come into conflict. In the case of Chile, legislation is still insufficient, due to the lack of an effective oversight body with adequate sanctions for some breaches of law. As a result Chile does not fully comply with the OECD guidelines or the standards of Directive 95/46/CE, making Chile an unsafe country for the flow of data according to EU.

8. REFERENCES

[1] Escobar, E., and Marulanda, L. *El Derecho a la Intimidad.*

[2] Gómez, A., *Auditoria de Seguridad Informática.*

[3] Greenleaf, G., Global Data Privacy Laws: 89 Countries, and Accelerating (February 6, 2012). Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012, Queen Mary School of Law Legal Studies Research.

[4] Hahn, R. W., and Layne-Farrar, A., The Benefits and Costs Of Online Privacy Legislation (October 2001). AEI-Brookings Joint Center Working Paper No. 01-14.

[5] Nash, V., and Peltu, M., Rethinking Safety and Security in a Networked World: Reducing Harm by Increasing Cooperation (November 1, 2005).

[6] Solove, D. J., A Brief History of Information Privacy Law. Proskauer on Privacy, PLI, 2006; GWU Law School Public Law Research Paper No. 215.

[7] Rajevic, (2010), Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación, Ponencia presentada en el taller "Chile y la Protección de Datos Personales", organizado por Expansiva (November 2010).

[8] Castillo, V. and Esquiaqui, (2013), Class Exercise on Internal Audit of Information Security.