Protection of personal data in private sector in Paraguay

An exploratory study

Luis Alonzo Fulchi
Maricarmen Sequera

TEDIC
TECNOLOGÍA & COMUNIDAD

Table of contents

Introduction....4
Background....4
Theoretical Framework....5
Personal data....5
Principles of Protection....5
Objective....6
Methodology....6
Sampling framework and cases of study....7
Categories of analysis....7
Analysis of findings....8
Conclusions....9
Bibliography....10

This research was made with the support of **Privacy International**, a United Kingdom organization that monitors invasions to privacy by governments and corporations.

Authors:

- Luis Alonzo Fulchi
- Maricarmen Sequera Buzarquis

Collaboration:

- Eduardo Carrillo
- María Bozzano

Introduction

The advance of digital technologies has generated multiple instances in which personal data are subject to automated processing by the public and private sector to perform commercial and state services quickly and effectively.

The protection of personal data protects people from every infringement of their rights due to the processing of their personal data. This right gives them the right to oppose any harmful processing of their personal data by third parties.

The absence or limited protection of personal data leads to practices that affect human rights such as privacy, freedom of expression, freedom of association and others. For there to be a balance between technology and human rights in Paraguay, it is essential to **diagnose** the current state of personal data processing in all sectors and then move to a broad and participatory debate among all the multiple stakeholders.

In this sense, from TEDIC we present this second part of the research on the protection of personal data for the year 2017. The first part included the status of the legal framework in force in the country and the management of personal databases in the public sector: the findings led to the rapid exploration and generation of similar questions on the databases of some companies in the private sector in Paraguay.

Regarding the interviews carried out, it should be noted that we took companies in the area of health and finance. In some cases the company is relatively small and in other cases we interviewed spokespersons of companies with personal data of millions of people, all of them from Paraguay.

Background

Paraguay is one of the few countries in the region that does not have a comprehensive Act on the protection of personal data (Acuña, Alonzo, & Sequera, 2017). Since the entry of Paraguay into the Organization for Economic Cooperation and Development (OECD) in January 2017[1] and the current negotiation of the free trade agreement between MERCOSUR and the European Union[2], the country is surrounded by international guidelines and standards on the protection of privacy and the cross-border flow of personal data that should adapt normatively to the volumes and multiple uses of personal data that are generated in a simple and increasingly low-cost way resulting from the collection, storage, processing, aggregation, analysis and transfer of such.

Given the lack of regulations of data protection in Paraguay, the business of selling personal databases of bank and financial loans has grown indiscriminately. Among the data sold illegally are IDs, number of mobile phones, police and judicial records and others, violating fundamental

[1] OECD. Paraguay becomes a member of OECD https://www.oecd.org/dev/paraguay-convierte-miembro-centro-desarrollo-ocde.htm [Date of consultation: 8 February, 2018]

[2] The observer. Repeated issue: Mercosur and EU did not close the FTA in Asuncion. Date: 2 March 2018. https://www.elobservador.com.uy/figurita-repetida-mercosur-y-ue-no-cerraron-acuerdo-tlc-asuncion-n1177396 [Date of consultation: 3 March, 2018].

principles of the protection of personal data such as consent and autonomy of people regarding their information.

In absence of the implementation of regulations, people are exposed to every type of problems and risks such as spam, invasive calls, extortion attempts, etc.

On the other hand, the figure of the *scapegoat* usually appears, as in the case of young people of the countryside[3], who distribute databases to credit companies and appear to be solely responsible of the problem.

It is important to point out that the sale of databases is only the emergent one: there is a strong responsibility in the collection, storage, crossing, disclosure and also in the purchase of these databases, and it is the State that does not have the ability to fulfill its role of *effective protection*, nor of sanctions to the responsible for leaks and abuses committed against personal databases.

Theoretical Framework

Personal data

For this research we will take the definition of personal data written in the new regulation on personal data of the European Union (EU) 2016/679:

> *"any information relating to an identified or identifiable natural person (the data subject); an identifiable natural person shall mean any person whose identity can be determined, directly or indirectly, in particular by reference to an identifier, for example a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of such person" (European Parliament, Council of the European Union, 2016).*

Principles of Protection

In addition, we will apply the same principles of the research of public sector databases to private sector databases (Banisar, 2011), as the highest standard and for which Paraguay must advocate for the effective protection of personal data. These principles are:

- Principle of **collection:** the collection of personal data shall be limited and have a specific objective. Data can only be collected through legal instruments with the permission of the data subjects, if necessary.
- Principle of **data quality**: data collected shall serve the purpose of their collection. They shall be precise and updated.
- Principle of **purpose specification**: the purpose of the collection of information shall be precise at the time of gathering the data. Such purpose shall guide the use of the data.

[3] La Nación. Citizen privacy for sale. Date 22 May 2017. Available at: http://www.lanacion.com.py/destacado_edicion_impresa/2017/05/22/privacidad-ciudadana-a-la-venta/ [Date of consultation: 18 February, 2018].

- Principle of **limitation in use**: personal data shall not be published, imparted or disclosed for reasons other than the purpose of their collection. The data subject shall expressly agree or authorize for the disclosure to be allowed.
- Principle of **security**: information collected shall be protected against possible risks such as loss, sabotage, destruction, etc.
- Principle of **openness**: there shall be a general openness policy on development, practices and regulations related to personal data. Ways of identifying the existence and nature of personal data and the main reason for their use shall be available, as well as the identity of the data controller and the storage place of the data.
- Principle of **individual participation**: a person shall have the right to:
    - Obtain from a data controller (or another person) a confirmation that the data controller has or does not have data related to the individual;
    - Obtain such information within a reasonable time at a price (or no cost at all) that is not excessive, in a reasonable manner and in a format that is intelligible to the person;
    - If the request for information is denied, obtain an explanation and have the possibility to appeal the denial;
    - Be able to request a correction of the information contained in the database, either by rectifying, completing, amending or deleting it.
- Principle of **accountability:** data controllers shall be accountable for adherence to measures which materialize the principles of personal data protection.

Objective

This second part of the research aims to complement the diagnosis of the state of databases of the main research, including three databases of the private sector in order to generate more information and more debate from a comprehensive and expanded view of the processing of personal data in Paraguay.

Methodology

It is the replica of the main research; it is exploratory, taking into account that at a local level there a few academic works that deal with the topic of personal data protection. As a reference for the analysis of the findings, the protection standards summarized in the work of David Banisar and the provisions of the new Regulation of the European Union (EU) 2016/679 will be used. The methodological tool to be used is the semi-structured interview.

The interviews seek to explore the situation of the processing of personal data in three private companies and seek to inquire about the amount and status of databases with personal data managed by these companies. The aim is to know the quantity and quality of such data, as well as the procedures used by the companies to manage such databases. In addition, to know how they are stored, updated, protected collected, etc.

The interviews last for at least half an hour and are anonymous in order to achieve a certain degree of trust in the interviewees and protect them against possible reprisals in their workplaces.

Sampling framework and cases of study

Four private companies were requested: one related to databases of the health sector, the other three related to the financial sector with different purposes such as loans, savings and tax payments through digital services.

On this last point, the company that offers digital services did not show interest in participating in the interview. Therefore the total number of companies interviewed was reduced to 3. At that point, the sample was considered saturated for the objectives set in the research.

Categories of analysis

Based on an interview script or guiding questions – available in Annex A.1. – a set of categories of analysis was elaborated and was enriched and improved during the same analytical procedure.

Analysis of findings

From the interviewed actors, we can infer that there is a great variety of situations in relation to personal data.

This variation is worrisome since there are cases of a total absence of protocols and standards, failing in the vast majority of "principles of protection" until almost a complete non-compliance.

An important and worrying finding is that companies usually collect information without **specific legal instruments** and in general without knowing the "good practices" in the collection, an element established in the **principle of collection** that we previously mentioned.

The same happens with the **principle of purpose**: about collection and purpose, companies usually justify them in the "need for the development of their mandate". Some companies specify their purpose in the **adhesion contracts**, although it is not clear at which level they specify it and if they then comply with this principle and **limitation of use.** An analysis of such contracts would be necessary to clarify whether this principle is respected or not in the cases that specify it, but it goes beyond the scope of this work.

Regarding the principle of **data quality**, the update and control of accuracy is usually done at times where users are in situ and it seems to be no systematic way of controlling that. Only one of the institutions affirmed a proactive willingness of updating the data from their databases.

In terms of security of information, which we call **principle of security**, it is worth introducing the standard ISO 27001. This standard, issued by ISO[4], was created in 2005 and specifies the requirements to manage the security of corporate information. It can also be applied to any type of organization.

Being certified with this standard implies having protocols and taking a series of measures and recommendations that this international consortium of experts established for the protection of the security of information. From the interviews, it appears that very few companies are certified with this standard, which are always the same companies that apply the rest of the principles, which means that the vast majority of companies do not have this certification and apply only some of the principles of protection. Risk management is done in a completely ad-hoc way.

It should be noted that as a general policy of the companies, all staff in charge or involved in the management of databases are fully identified in the actions they carry out and have permits according to the needs of their roles and nothing else. However, this measure seems to be insufficient given the amount of databases with personal data that circulate in the illegal market of our country.

Regarding **transfer**, there is usually only specific data query, that is, the remote execution of a script that allows to obtain only concrete and specific information on individual records and not the information in the form of a database. That said, companies declared that they do not have mechanisms or protocols to transfer databases at national or international level.

[4] ISO is the International Organization for Standardization, founded in 1947 and is recognized by the Economic and Social Council of the UN.

As regards **limitation of the storage** period, all interviewed companies said they do not **destroy data**, that is to say they keep it for an unlimited time.

The delivery of information of **criminal prosecution** to the authorities is not standardized either. In some cases they claimed to deliver the information with a prosecutor´s note, instead of the due process of a court order issued by a judge. In this regard, an interviewee said:

> *"In general, confidential information is delivered under a court order"*

The part of the phrase that says "in general" is worrisome since, in some way, shows that there are cases where confidential information may be delivered only with a prosecutor's note, as we mentioned.

Except in one of the cases, it is confirmed that the same thing has been found for the public sector and is that the **units in charge of IT** are usually small. These units are the ones responsible for storage, backup and protection infrastructure for databases with personal information.

Conclusions

There is a complete **heterogeneity** of situations concerning the protection of personal data in a legal, human and technological level. Very few companies have approved the ISO 27001 and some others have barely developed protocols and good practices. That is, there is **discretion** in the protection of such bases.

There is practically no adherence to the **international standards** of protection of databases that were developed in the introduction and in the theoretical framework of the research of public databases in Paraguay (Acuña et al., 2017).

Paraguay has serious risks of **cyber-attacks** by national or foreign agents as it has happened in numerous occasions. This is much more complex and risky for the safety and privacy of people, in the context of the massive collection of personal data by both private companies and public sector bodies.

In this sense, there is some distrust and a certain fear of the private sector when it comes to sharing information on the **cyber-attacks** they suffer. This must be addressed in the context of the National Cyber-security Plan (CERT, SENATICS, 2016), since a warning and information exchange system on the attacks becomes essential to strengthen the rest of the companies and institutions against such attacks.

The imperative need for the **creation of an Organic Act on Personal Data** is evident (several of the interviewees emphasized this). It is necessary to generate pluri-participatory discussion areas which allow determining better practices to face the challenges associated with the defense of the right of protection of personal data at a global level.

Bibliography

Acuña, J., Alonzo, L., & Sequera, M. (2017). Protection of Databases in Paraguay. *September*, *2017*, *1*(1). Recovered from https://www.tedic.org/wp-content/uploads/sites/4/2017/09/La-protecci%C3%B3n-de-Bases-de-Datos-en-Paraguay_Documento-Final.pdf

Banisar, D. (2011). The right to information and privacy: Balancing rights and managing conflicts. *The World Bank*, *Access to Information Program*. Recovered from https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf

CERT, SENATICS. (2016, November 9). National Cyber-security Plan. Recovered from http://gestordocumental.senatics.gov.py/share/s/m2uDswEUTDmrDBY2NFttIg

European Parliament, Council of the European Union. (2016, April 27). Regulation (EU) 2016/679 of the Euripean Parliament. Recovered from http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

"I don't want to live in a world where everything that I say, everything I do, everyone I talk to, every expression of creativity, or love, or friendship is recorded" Edward Snowden