Protection of personal data in public databases in Paraguay

An exploratory study

Jazmín Acuña
Luis Alonzo Fulchi
Maricarmen Sequera

TEDIC
TECNOLOGÍA & COMUNIDAD

Table of Contents

Introduction 4

Theoretical Framework 5

Definitions of Concept 5

Public information 5

Public databases 5

Personal data 6

Right to Access to Public Information / Right to Privacy 6

Principles of personal data protection 7

Purpose of the Research 10

Methodological Strategy 11

Justification of the methodological choice 11

Sampling framework 11

Categories of analysis 12

Cases of study 12

Legal analysis of the National and International Legislation 13

The National Constitution and International Treaties 13

Habeas Data 14

Private Information – Act 1682/2001 and amendments 14

Principles of Personal Data Protection 16

Penal Code 20

Code of Judicial Organization 20

Act 642/95 of Telecommunications 20

Resolution 1350/2002 By which the Obligation to register the call detail record for a period of six (6) months is established 21

Resolution 1350/2002 By which the Obligation to register the call detail record for a period of six (6) months is established 21

Electronic Commerce Act and its regulatory decree 21

General Act 861/96 of Banks, Financial and other credit institutions: 23

Act 125/1991 That establishes the New Taxation Regime 23

Resolution N° 77/16 of the Secretariat for Taxation – Ministry of Finance 23

Access to Public Information Act 24

The Act “That prohibits unauthorized advertising by the users of mobile phones” 25

National and International Jurisprudence 26

IACHR: Case of Escher et al. v. Brazil....26
Sentence of the Supreme Court N°674/10, The Case of Cecilia Cubas....27
Ricardo Canese vs. Paraguay (Funds, Reparations and Court Fees)....28
International Instances....28
International Instances....28
Common Market of the South....28
Organization of American States....29
Ibero-American Data Protection Network (RIDP)....29
Ibero-American Data Protection Network (RIDP)....29
Organization for Economic Cooperation and Development....29
United Nations....29
Analysis of Interviews....31
Personal data in databases of public sector bodies....31
Nature of Databases....31
Examples of databases....33
Principle of collection....34
Principle of purpose specification....36
Principle of limitation in use....37
Principle of data quality....37
Principle of conservation....38
Principle of Safety....38
Conclusions and recommendations....41
On the creation of an Act for personal data protection....42
Bibliography....43
Bibliography....43
Annexes....46
A.1. Interview Script....46
Nature of databases....46
Application of protection principles....46
Regulations, protocols of use and processing of databases (principle of security)....46
Authorization of access and transfer to the bases....49

Introduction

This research seeks to explore the status of protection of personal data stored in databases in some public sector bodies in Paraguay. Specifically, to identify the uses, management, procedures, risks, regulations and legislation that govern the management of such databases.

For the research, a legal analysis of the current national legislation was carried out, as well as the international legislation and jurisprudence that is binding for the country. In addition, 9 cases were studied, that is, 9 public sector bodies which manage databases with personal data, which are: Technical Secretariat for Planning (STP), Ministry of Public Health and Social Welfare (MSPBS), National Computing Center (CNC), Secretariat for Social Action (SAS), Ministry of Industry and Commerce (MIC), National Customs Office (DNA), Sub-Secretariat of State for Taxation (SET), National Secretariat for Housing and Habitat (SENAVITAT), and the Ministry of Education and Science (MEC).

The theoretical framework of the research is based on legal literature, science of information, international treaties, legislation, rules and local regulations in force. The methodological framework is qualitative: legal analysis and semi-structured interviews. Regarding the interviews, they were carried out with qualified informants, authorities and civil servants of public sector bodies in charge of the databases processing.

This research seeks to establish what principles and standards of protection do public sector bodies apply in the management of databases that contain personal data. In addition, it seeks to provide an initial analytical input for the design of public policies regarding the protection of personal data.

The research is divided into five chapters. The first chapter contains the theoretical framework in which the main concepts of the study are developed, a brief commentary on the tensions existing between the rights to access to public information and the protection of personal data and the standards of protection of personal data. In the second chapter, the goals and the methodological framework are detailed, along with the presentation of the guiding questions of the research and the selected case studies for the interviews. In the third chapter, the analysis of the normative framework of Paraguay is presented. In the next one, the findings from the interviews of the 9 case studies are detailed. These findings are measured with indicators related to the internationally agreed protection standards. Finally, the last chapter provides a conclusion and recommendations for public policies.

Theoretical Framework

Definitions of Concept

In the discussions on protection of personal data in databases of public sector bodies, the following concepts are used: *public information*, *public databases*, and *personal data*, among others. The definitions of these concepts are relevant since they serve to better understand the scope and challenges of the matter. An approach of these concepts, which are the base of this research, is now presented:

Public information

International organizations and academia have established definitions of what *public information* is. The Inter-American Court considers that article 13 of the American Convention on Human Rights protects the rights of individuals to access public information. It specifies that this information is the one that "is under the control of the State".

Directive 2003/98/EC of the European Parliament and of the Council of the European Union of 17 November 2003, on the re-use of public information, established some definitions of what such information constitutes (EUR-Lex 2003) [2]. In its article 2, it details what the re-use of public information means, specifying what public information is: *"[...] documents held by public sector bodies [...]"* [3]. In paragraph 3 of the same article it explains that *document* means: *"any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording)"* [4].

For its part, the Organization for Economic Cooperation and Development (OECD) establishes that *information and content of the public sector body* is any type of information produced and/or collected by public sector bodies, and forms part of the role assigned to the body [5].

Raed M. Sharif, a professor and researcher at Syracuse University, in a dissertation on the use and value of public information for the creation of knowledge, considers that public information is composed of:

> *"data and information produced by or for public sector bodies which include, for example, data of education and health, geographical data, financial reports, social and economic statistics, legislative and judicial procedures, data of water and food resources, and many other types of data and information, and which collectively are referred to as 'public sector information'" [6].*

From the principles contained in the definitions of *public information* it could be inferred that all information held by the State is public and therefore must be accessible. However, the principles of personal data protection, which are detailed later in this research, limit such access. Therefore, the processing of public databases which contain personal data must be made taking into account such principles.

Public databases

Due to ambiguities in the law on "Private Data" (National Congress, 2001) in Paraguay, it is worth focusing on the definition of databases and, in particular, in those which are held by State institutions:

> *"[...] an organized set of data which are managed or processed, electronic or not, regardless of the type of formation, storage, organization or access, whose owner is a legal person of public nature".*

From this definition, we observe that a set of data stored in an organized paper filing, in drawers of a public sector body, are also databases. But the main interest of this research are the ones that are digitalized.

Personal data

To specify the concept of personal data, it is possible to use the Madrid Resolution [8] of 2009, where a *Joint Proposal for a Draft of International Standards on the Protection of Privacy* is established, with regard to the *Processing of Personal Data*. Personal Data is defined therein as:

> *"any information relating to an identified natural person or a person who may be identified by means reasonably likely to be used" [9].*

The Regulation of the European Union (EU) 2016/679[1], on the protection of natural persons, regarding the processing of Personal Data and its free circulation, *expands the definition* to adapt it to the new challenges imposed by technological advances. In the new Regulation, personal data is considered as:

> *"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" [10]*

Other concepts relevant for this study will be outlined in the presentation of the *general principles* that govern the *Personal Data protection* in databases. Before that, it is necessary to recognize the tensions and limitations existing between the right to access to information and the right to the privacy of people, through the protection of personal data.

Right to Access to Public Information / Right to Privacy

The topic of databases with personal data, whether public or private, is in the middle of tension between two rights: the right to access to public information and the right to the privacy of people.

The right to information derives from the right to expression of freedom expressed in article 19 of the Universal Declaration of Human Rights:

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (UN, 1948)*

The *American Convention on Human Rights of the Pact of San Jose from Costa Rica*, in article 13 on the "*Freedom of thought and expression*", establishes the right of people to "*seek, receive and impart information and ideas of all kinds*"(OEA, 1969). It is important to note that the same article also establishes the limits to this right, understood as ulterior responsibilities. It specifies that these limits must be expressed by the Act to ensure "*a) respect for the rights or reputation of others; or b) the protection of national security, public order or public health or morals*".

On the other side, the right to privacy is recognized as a universal right in article 12 of the Declaration. It is understood as the right to "private life". It expresses:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." (UN, 1948)*

[1] This repeals Directive 95/46/CE

This right has also been recognized in other international treaties and local legislations with some variations. David Banisar relates it "*to the protection of individual autonomy and the relationship between the individual and society, including governments, companies and other individuals*"(Banisar, 2011). He distinguishes 4 dimensions which are useful to understand the breadth of the concept, among them the *informative privacy, "which involves the rules to manage personal data".* This is the dimension that will be explored in this study.

Conflicts between *access to information* and *privacy* exist because much personal information is in the hands of the government. Banisar mentions some resolutions about it. For example, he explains that there is consensus that information of elected candidates has less guaranties of protection. Also, personal information of civil servants generated in their official capacities is not necessarily subject to protection. However, there are other examples which evidence disagreements or dissent. In European countries, governments keep reserved all information of people who are part of social support programs. On the contrary, in countries of the southern hemisphere, this information is public so as to avoid cases of corruption and for the social monitoring of these programs. There is no agreement on the management of judicial records.

In a study on Chilean legislation, Renato Jijena proposes some ways to resolve some tensions between the processing of personal data in public sources and the right to access to information, expressed in Act 20.285. To his criteria,

"the processing of personal data of citizens is and should be legal and constitutionally limiting to the exercise of the right of access to acts, contracts, documents, resolutions and procedures of the State Administration"(Jijena, 2013).

Jijena raises the need to carry out a study "case by case" when it comes to conciliate the right to access to information and the personal data protection. He warns that the protection of personal data should not be used in a "general and systematic" way so as not to open information from the State. If so, corruption cases could be protected and go unpunished.

Principles of personal data protection

For the protection of personal data, International organizations, academia and governments have worked and established principles and standards for the processing of such data. David Banisar synthetizes these principles in a work on the right to access to information and the right to privacy (Banisar, 2011), which are detailed below:

- 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.
- 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:
    a) Obtain from a data controller (or another person) a confirmation that the data controller has or does not have data related to the individual;
    b) 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;
    c) If the request for information is denied, obtain an explanation and have the possibility to appeal the denial;
    d) 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.

The Regulation of the European Union (EU) 2016/679 (European Parliament, Council of the European Union, 2016), which is one of the most recent regulations on Personal Data protection, includes in its article 5 a series of principles regarding the processing of such data. The principles established therein are mostly the same as those presented above. However, they are mentioned now as a reference for this research and the subsequent analysis of the findings:

- **Lawfulness, fairness and transparency**: personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation**: the Regulation says that personal data shall be collected for "specified, explicit and legitimate purposes". They shall not be further processed in a manner that is incompatible with those purposes. The Regulation expresses that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes of the collection.
- **Data minimization**: the Regulation expresses that personal data shall be "adequate, relevant and limited" to what is necessary in relation to the purposes for which they are processed.
- **Accuracy**: personal data shall be kept up to date, according to the Regulation. It specifies that every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage limitation**: the Regulation establishes that personal data shall be kept in a form which permits identification of data subjects "for no longer than is necessary for the purposes for which the personal data are processed". Personal data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) of the Regulation.
- **Integrity and confidentiality**: personal data shall be processed in a manner that ensures appropriate security of the personal data including, according to the Regulation, "protection

against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures”

- **Accountability**: article 5 (2) refers to the person responsible for the data processing. It states that the controller shall be responsible for, and be able to demonstrate compliance with paragraph 1.

Purpose of the Research

The purpose of this research is to generate an input of information and analysis to strengthen the norms and practices of personal data protection contained in public databases in Paraguay.

Specifically, the research aims at laying the necessary argumentative bases to design a reform proposal for the Act of personal data protection. Update the current legislation to the challenges imposed by new technologies is imperative to safeguard the rights of millions of citizens. In addition, as Act 5282/14 of free access to public information is being implemented, tensions arise with the need to protect personal data and the protection of the privacy of people. Such tensions arise due to the absence of clear regulations, resulting in situations in which civil servants decide what to do in each case, according to their criteria.

A secondary purpose of the research is to provide a document which can be useful to produce more academic works related to the topics mentioned herein. It is necessary to expand the repository of knowledge in this area. At the moment, no local studies have been found on personal data protection, public databases, right to privacy and other topics which are investigated in the present research.

To reach the main purpose of this study, the uses, managements, procedures, risks, regulations and legislations which define the processing of databases that include personal data in the public sector bodies are identified. A legal analysis on the country's current regulation is carried out. On the other hand, interviews are also carried out to employees in charge of databases in nine public sector bodies to investigate what principles and standards of protection they apply in the management of such databases.

The results of the research are shared in the communication channels of the organization and are delivered to the State authorities who have the capacity to promote changes in the norms and practices of personal data processing in public databases.

Methodological Strategy

Justification of the methodological choice

The research is of exploratory nature, taking into account that, at a local level, there are few academic works that deal with the topic of personal data protection. There are no previous theories to refute or reaffirm with the findings of this research. Nor there is a hypothesis to prove or discard. What is sought is to know the status of the processing of personal data in public databases in Paraguay. As a reference for the analysis of the findings, the protection standards summarized in the work of David Banisar and the stipulations of the new Regulation of the European Union (EU) 2016/679 will be used.

There will be an exploratory approach using 2 methodological tools. On one hand, a legal analysis that will serve as an input for the rest of the research. This analysis will allow us to have a conceptual framework on the processing of personal data while it will also serve to establish a sort of legal "state of the art". The second methodological tool –semi-structured interviews- comes from qualitative methodologies.

The interviews seek to explore the situation of the personal data processing in public sector bodies and to know where some of the databases of the current administration are and what the status of the data contained therein is. For this research, we explored the possibility of carrying out interviews in the private sector, but due to its variety and quantity, as well as possible methodological problems of these kinds of instruments, we decided to limit our sampling frame and to take only public entities from the central administration.

In addition, we carried out *two interviews with qualified informants* in order to construct the theoretical sample and to find those public sector bodies with the most important and most vulnerable databases. These interviews provide an overview on the processing of databases in the private sector which, as mentioned before, is much broader in terms of diversity of actors and more complex regarding veracity and convenience of the interviewees' answers. To pretend that private companies will respond unreservedly the questions foreseen in the interviews script would be of little methodological rigor.

Interviews with public sector bodies seek to inquire on the quantity and status of the databases with personal data which are managed by certain areas of the public administration. That is, to know the quantity and quality of such data, as well as the procedures used by each institution to manage such databases. Moreover, to know how they are stored, updated, protected and how such data are collected, etc.

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

Sampling framework

Based on the interviews with civil servants and qualified informants, we constructed a theoretical sampling framework containing the following institutions: Technical Secretariat for Planning (STP), Ministry of Public Health and Social Welfare (MSPBS), National Center of Computing (CNC), Secretariat for Social Action (SAS), General Department for Surveys, Statistics and Census (DGEEC), National Department of Identifications, Ministry of Industry and Commerce (MIC), National Customs Office (DNA), Sub-Secretariat of State for Taxation (SET), Center of Answers on Cybernetic Incidents (CERT), Central Bank of Paraguay (BCP), National Secretariat for Housing and Habitat (SENAVITAT), Ministry of Education and Science (MEC).

As the interviews progressed, from the difficulties and possibilities of contacting the interviewees, the number of institutions was reduced to 9. At that point, the sampling was considered saturated for the purposes set in the research.

Categories of analysis

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

The pre-defined categories are divided into 3 preliminary sets which are then broken down in the following way:

Principles of protection:

- Collection
  - Notification
- Purpose
- Limitation in use
- Quality
- Storage

Access and transfer:

- Levels of access
- National transfers
- International transfers

Infrastructure:

- Cyber security
- Good practices
- Human resources for sustainability

Cases of study

Nine cases were studied, that is, 9 public sector bodies which manage databases with personal data, which are: Technical Secretariat for Planning (STP), Ministry of Public Health and Social Welfare (MSPBS), National Center of Computing (CNC), Secretariat for Social Action (SAS), Ministry of Industry and Commerce (MIC), National Customs Office (DNA), Sub-Secretariat of State for Taxation (SET), National Secretariat for Housing and Habitat (SENAVITAT), Ministry of Education and Science (MEC).

It should be noted that the initial number of institutions which were sought to explore was greater. However, as the interviews were being carried out, from the difficulties and possibilities of contacting the interviewers, the number of institutions was reduced to 9. At that point, the sampling was considered saturated for the purposes set in the research.

The databases which are managed by the 9 studied institutions are specified in the section of the interviews findings. That section includes the decrees or regulations of establishments of each body, the data that databases collect and what personal data they contain, in addition to the limitations or protection practices that those responsible for them apply to keep them safe.

Legal analysis of the National and International Legislation

The following is a legal analysis of the current national legislation that protects the privacy of people and is directly related to the purpose of our study, which are the databases containing personal data in the country.

The National Constitution and International Treaties

At an international level, there are a number of treaties which expressly contemplate the protection of private life, for example, the Universal Declaration of Human Rights (UN, 1948), in which article 12 points out that nobody shall be subjected to arbitrary interference with their privacy, which is reflected in the International Covenant on Civil and Political Rights of the United Nations (Art. 17 (1)) (UN, 1966) and the American Convention on Human Rights (Art. 11 (2)) (OAS, 1969). All of these treaties and conventions have been ratified by Paraguay, which means that they become part of its national legal system.

In the constitutional reform of 1992, the following figures are incorporated to the National Constitution (CN) (Constitutional Assembly, 1992):

> *Art. 33 – On right to Privacy – "Personal and family privacy, as well as the respect for private life, are inviolable. The behavior of people, as long as it does not affect the public order established in the law or the rights of third parties, is exempt from public authority.*
> *The right to protection of privacy, dignity and public image of people are guaranteed"*
> *Art. 36 – On inviolability of documentary heritage and private communication: "The documentary heritage of people is inviolable. Records, whatever their technique, printed ones, correspondence, written, telephonic, telegraphic or any other type of communications, collections or duplicates, testimonies or objects of testimonial value, as well as their respective copies, cannot be examined, reproduced, intercepted or seized without a judicial order for cases specifically stipulated in the law, and provided they are indispensable for the clarification of the matters of competence of the corresponding authorities. The law shall determine special modalities for the examination of commercial accounting and mandatory legal records.*
> *Documentary evidence obtained in violation of the above provisions, shall not have any value in a trial. In all cases there shall be strict caution on what is not related to the investigation."*
>
> *Art. 23 – On proof of truth – "The proof of truth and notoriety shall not be admissible in the processes brought about by publications of any nature which affect the honor, reputation or dignity of people, and that refer to crimes of private penal action or private behaviors that this Constitution or the law declare exempt from public authority. Such evidence shall be admitted when the process is promoted by the publication of censures to the public behavior of State employees, and in other cases established expressly by law."*
>
> *Art. 28 – Right to be informed (final paragraph): "(...) Every person affected by the disclosure of a false, distorted or ambiguous information has the right to demand its rectification or clarification by the same means and under the same conditions as it has been disclosed, without prejudice to other compensatory rights".*

As it can be observed, Paraguay has a strong constitutional protection for privacy and inviolability of people's communication, as well as the right to informational self-determination.

Regarding privacy, the only precedent of protection in our country corresponds to the time of the totalitarian regime of Alfredo Stroessner and was in the 1967 Constitution, amended in 1977. In its article 50, it mentioned "the protection of honor and reputation" (Pappalardo Zaldivar, 1992).

Habeas Data

The right to data protection has constitutional recognition. Article 135 of the 1992 CN establishes the guarantee of habeas data, which provides as follows:

> *"All people can access the information and data about themselves or about their properties, which are found in private or official records of public nature, as well as to know the use made of them and their purpose".*

In addition, people may require the update, rectification or destruction of personal data which are erroneous or that illegitimately affect their rights before competent authorities.

The first case in which this guarantee was used was in 1992 when the lawyer Martín Almada, defender of human rights and a political exiled, requested access to his data stored in the files of the Stroessner dictatorship[2].

Currently, the action of habeas data is promoted before a judge of first instance, and the national jurisprudence on this matter is vast. Curiously, most of the actions are promoted to eliminate personal data of judicial cases which have ended[3]. Nowadays, this personal data elimination was modified by the act which Regulates Private Information (1682/2001) (National Congress, 2001).

Constitutional protection is not enough, due to ambiguous or misleading judicial interpretations or absence of *Stare decisis et non quieta moveré*[4] of judicial sentences, inefficiency in the prevention of breaches and transactional costs. For all this, it is necessary an *in extenso* regulation which includes informational self-determination[5].

Private Information – Act 1682/2001 and amendments

Data subjects –which are conceived as natural persons in respect of whom certain information is given– may go to court to exercise their constitutional rights through habeas data or other rights of protection against infringements committed against them. But the most important part of the discussion is “the need or not for the State to adopt an Institutionality which ensures compliance of the regulation on the processing of personal data and that it is not left only to the management of the agents involved”. That is, that the State generates mechanisms and guarantees for the processing of personal data.

In Paraguay, personal data are regulated by Act N° 1682/2001 (National Congress, 2001) “Which regulates private information” and its subsequent amendment[6] by Act 1969 of year 2002 (National Congress, 2002) and 5.543/2015. Such Act assumes that the action of protection is under the responsibility of the affected person, being closer to the North American doctrine which implies

---

2 These files, once recovered, included more than 700.000 records of interrogations, tortures and State surveillance. This record was named "Archive of Terror", currently declared as intangible heritage of humanity by the UNESCO.

3 See jurisprudence finder of the Supreme Court of Justice: http://www.csj.gov.py/jurisprudencia/default.aspx?AspxAutoDetectCookieSupport=1

4 It is translated interpretatively as "to stand by decided matters", used in law to refer to the doctrine according to which sentences passed by a court create a judicial precedent and link as jurisprudence those that, on the same subject, are passed in the future.

5 According to Rodriguez Palop, the "*Right to informational self-determination (…) has a double dimension, an individual or negative one, formulated as the right to the privacy of the private life which seems to approximate to the rights of first generation of an individualist nature and are inspired by the value of freedom, and the second is a social or positive dimension, as it requires a greater participation of citizens, a control by them of the information and communication technologies, and an extension of their real possibilities to interfere in social and economic processes in equal conditions, it may resemble a right to political participation derived from the freedom to be informed*" (Rodriguez Palop & Universidad Carlos III de Madrid, 2002).

6 There is a document with the complete process of the Act in this link: https://www.informconf.com.py/docs/Comparativo_ley_1682-01_y_modificatorias.pdf

leaving the compliance of the norm to the parties involved and avoid the intervention of the State, except when it comes to the role of the courts of justice.

This option does not contemplate the qualification standards of personal data protection of the European Union Directive 95/46 (European Union, 1995) and the new general regulation of personal data protection of the European Union 2016/279[7], especially the figure of informational self-determination. It is also observed that there are no legal definitions of "personal data", "data processing" and "data subject".

Act 1682/2001 (and its amendments) has a purely economic approach since it regulates almost exclusively credit information systems in banks and financial institutions, without involving social and communitarian approaches of personal information. It currently consists of 12 articles of which 5, 7, 9 and 10 regulate credit reports. However, for the analysis of this current Act we used the principles advocated by the European system of personal data protection.

In the following section there will be a thematic breakdown and a legal analysis of such Act and its amendments.

Effective Guardianship

The figure of effective guardianship is not contemplated in Act 1682/2001 since, as explained above, the protection is not carried out ex-ante by the State.

One of the achievements of the current Act is that the sentences of the Judicial Branch are limited to delete information under the figure of "right to be forgotten" after the time of disclosure of personal data and not through *habeas data*, as it was done previously[8].

Scope of application

The scope of application of the Act is the management of private information in general, regardless of how it is carried out: "in files, records, data bank or any other technical medium for private or public data management, destined to give reports" (Art. 1). However, it specifically excludes databases of its scope of application, which is currently the most massive and generalized way of data storage.

The drafting of article 1 creates confusion since, on the one hand, affects data banks but excludes databases and in no case defines what is one or the other thing. According to the Royal Spanish Academy, a data bank is "a data file referring to a determined subject, which can be used by several users", while database is "a set of data organized in a way which allows to rapidly obtain several kinds of information". As it can be seen, and since they are not defined as one concept or another, the Act practically falls into a contradiction.

If we interpret that the Act excludes databases, it produces a contradiction with the concept of "informational self-determination". That is, it is necessary to provide the individual with faculties that go beyond the simple pursuit of economic compensation and give them also instruments of action which allow them to control and determine the destination or other aspects of the processing of their personal data. This Act does not contemplate the right that seeks the enjoyment of privacy and that comprehends the will of individuals to determine the purpose for which their data will be used, as well as the treatment that will be given to such in public and private registries stored mainly in digital media.

To exclude databases of the legal protection can show a lack of political will at that moment or a complete lack of knowledge of the potentialities of their use. This negligence exposes people to be

7 http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

8 See related sentences against Informconf on habeas data: http://www.pj.gov.py

individualized through their personal data, which causes an invasion of privacy that should be protected. This has caused the proliferation and business of databases of private or sensitive information, disclosed without consents and for commercial purposes. In addition, another risk is the existence of cross-references and storage through what is known as Big Data[9], putting the population at risk, individualizing even more and giving space to possible discrimination against them.

It should be added that the Act lacks guarantees regarding the transfer and communication of data to third parties and does not contemplate provisions regarding the international transfer of data.

Principles of Personal Data Protection

The European Directive of Data Protection of 1995 is qualified as the highest standard in matters of data protection. Therefore: the criteria of the directive have been used to analyze the local regulation.

Principle of Collection

The purpose of the Act is in article 1 of Act 1682/01, amended by Act 1969/02:

> *Art. 1° - "The purpose of this Act is to regulate the collection, storage, distribution, publication, modification, destruction, duration and in general, the processing of personal data contained in archives, files, data banks or any other technical medium for processing of public or private data destined to give reports, in order to guarantee the full exercise of the data subjects' rights. This Act shall not apply in any case to the databases or sources of journalistic information or the freedom to express an opinion and to inform".*

The following is a series of elements that refer to the data processing and are observed in Act 1682/01 as amended by Acts 1969/02 and 5543/2015:

- It is allowed that any person can process personal data, provided that it is exclusively of private use (art. 2)
- Authorization of the data subject is not required when the data processing comes from public sources (art. 2)
- The law considers the publication of such data to be lawful when it is "carried out for scientific, statistical, survey and public opinion polling or market research purposes, provided that people or institutions investigated are not identified" (art. 3)
- When the "personal data subject" is mentioned, reference is made to the personal data of the natural person that includes sensitive data inherent to the natural person (art. 4) but excluding the category of legal persons[10]. The processing of sensitive data is not expressly prohibited.
- The data subject has the right to require the data controller to modify, cancel, block and delete his data (arts. 7 and 9)
- The responsibility lies with the data processor, that is, who collects, stores and keeps the data and assumes compensation for pecuniary and moral damages in the event of wrongful processing (art. 10)
- The purpose of the act explicitly excludes databases, journalistic sources and freedom to make an opinion and to inform (art. 1). It should be clarified again that there is a confusing distinction between data banks and databases.

Article 1 of the present Act highlights the data processing as the main purpose of the regulation of the Act. However, it does not distinguish between data collection by public and private sector

---

9 Big Data is the capacity to apply algorithmic analyses to growing volumes of information that both companies and governments collect of people, allowing to infer, through correlations, useful information not explicitly contained in such databases.

10 Even though in the Act these concepts are not clearly differentiated, it is interpreted in such way since in art .4 sensitive data are considered those regarding ethnical or racial, political or religious information, private image, among others, which are inherent to the natural person.

bodies. It does establish the rules for the data processing in the public sector, establishing that public sources of information are of free access, without limiting the personal data processing to the subject of its competence, nature and duration of such.

In this sense, in its article 2, the Act states that:

> *"Every person has the right to access the data contained in public registries, including those created by Act 879/81 and Act 608/95 and their amendments"*

The preceding article allows the access to *private information* by the data subject; however, it does not contemplate the security mechanisms in the operations of the data processing. Neither it is established the obligation of the data controller to protect them with due diligence, taking responsibility of the damages caused -in case the subject expressly gives consent for the records.

Principle of Purpose and Limitation of Purpose

The current Act lacks the principle of purpose on the use of collected data, which means the norm should establish the purposes for which the data have been collected. That is, the processing of personal data must be true, adequate, pertinent and not excessive in relation to the scope and purpose for which they have been obtained.

On the other hand, the same Act considers lawful any collection, storage, processing of personal data for private use exclusively (art. 2) and it only contemplates their publication when "it is carried out for scientific, statistical, survey and public opinion polling or market research purposes, provided that people or entities investigated are not identified" (art. 3). That is, it limits the principle of purpose by considering exceptions with the initial purposes of the collection.

Principle of Integrity and Confidentiality

The present Act does not contemplate legal security against unauthorized or illicit processing or against loss or destruction or accidental damage. The only current measure falls under the responsibility of the affected party or data subject, through the constitutional guarantee.

Principle of Accountability

Both public and private sector that carry out data processing must be subject to accountability on the measures they take for the processing of personal data. In absence of a specialized body which guarantees the compliance of accountability, transparency and the application of the standards in this Act, this principle is absent in the Paraguayan legislation.

Principle of Safety and Openness

These principles are not found in the present Act either. The collected information must be protected against possible risks such as loss, sabotages, destruction, etc. Currently, The National Cyber Security Plan (CERT, SENATICS, 2016)[11] includes a series of standards for the protection of the infrastructure which stores databases to technologically avoid these events; however the protection lies in the infrastructure and not in the person[12].

On the other hand, regarding openness, there are no public policies on the opening of information which is related to the development, practices and regulations in relation to the processing of personal data.

---

11 The National Cyber Security Plan is available at: http://gestordocumental.senatics.gov.py/share/s/m2uDswEUTDmrDBY2NFttIg

12 See article with comments on the National Cyber Security Plan in Paraguay at: https://www.tedic.org/aspecto-positivos-y-negativos-del-plan-de-ciberseguridad-en-paraguay/

Data categories

Each of the categories which the Act defines in terms of the characteristics of the data is analyzed as follows:

Personal data of public nature: The main characteristics of personal data of public nature are specified according to the Act (art. 6) which can be “published and disseminated a) Data consisting only in name, surname, ID, address, age, date and place of birth, marital status, occupation or profession, place of work and work number”.

Sensitive information: The Act contemplates the definition of sensitive information, adapting to international doctrine and jurisprudence that seek to prevail the right to privacy and the respect for sensitive information (art. 4). These are: “racial or ethnic affiliation, political preferences, individual health status, religious, philosophical or moral convictions; sexual intimacy and, in general, those which promote prejudices and discriminations, or affect the dignity, privacy, domestic intimacy and private image of people or families”.

Concerning sensitive data, their publication or disclosure is forbidden, but no sanctions are observed in case of abuse by any public or private institution. Therefore, the action of defense against an abuse is exclusively in the hands of the affected person.

From the above mentioned it is deduced that for the Act, there are personal data of nonpublic nature, that are not sensitive either, such as private telephone number, mobile number, height, blood type, etc.

There are also two other data categories, but which are not clearly defined: *outdated data and statistical data*[13]. The first one is the one which has lost relevance due to the provision of the Act, compliance of the condition or expiration of the term established for its validity, changes of the facts or circumstances it mentions if there is no express rule. On the other hand, a statistical data is the one which cannot be associated to an identified or identifiable subject. The latter one is out of the scope of the current standards of data protection, leaving free interpretation and a lot of vulnerability for the effective protection of the privacy of people.

Principle of Data Quality

The requirement of quality of data is part of the guiding principles of the Act and is in the article. But again, it is limited to credit reports such as assets, economic solvency and compliance of commercial and financial obligations, thus forcing constant updating by companies.

Article 7 of Act N° 1682/2001, as amended by Act N° 1969/2002, provides, in the final paragraph, as follows:

> *"In case the personal data were erroneous, inaccurate, equivocal or incomplete and thus credited, the affected shall have the right to have them modified. The update, modification or elimination of the data shall be absolutely free of charge and, at the request of the affected party and at no cost, an authenticated copy of the altered record in the pertinent part shall be provided".*

In relation to this, the ARCO rights are explained below:

---

[13] According to Alberto Cerda, an outdated data is "*data which has lost relevance due to the provision of the Act, compliance of the condition or expiration of the term established for its validity or, if there was no express rule, by the change of the facts or circumstances it mentions.” On the other hand, a statistical data is "data which, in its origin or as a consequence of its processing, cannot be associated to an identified or identifiable subject. The latter one, therefore, is out of the scope of application of the Act"* (Cerda Silva, 2011).

Principle of individual participation: ARCO rights

The concept of ARCO rights refers to the rights of access, rectification, cancelation and opposition on personal data. In the current Act, they are exclusively applied to credit information systems in banks and financial institutions. Any other exercise outside this area shall be carried out through the habeas data procedure. Although this Act does not contemplate the legal definition of "Data subject", it does consider the rights to the data subject as in the ARCO rights.

The right to access (or to information) is in article 8 of the Act, which provides the following:

> *"All people may have access to information and data about themselves, their spouses, people under their custody or guardianship, and their assets contained in official or private records of public nature or in institutions that provide information on economic solvency and patrimonial status, as well as to know the use made of them or their purpose".*

ARCO rights are very personal[14], which indicates they must be exercised by the subject of rights or by its legal representative, but in article 8 it is established that any person may request information about their spouse, causing confusion when it comes to interpret this right as very personal.

There is also a lack of requirement of express consent: a main and very personal right of the personal data subject. This implies that every person shall be informed about the purpose for storing their data and their eventual publication. In addition, there must be an express and/or written authorization, and can be revoked without need of a justified cause (without retroactive effect).

The right to rectification and cancellation[15] is observed in article 7 of the Act, amended by Act nº 1969/2002 and expresses the following:

> *"Personal data on the patrimonial status, economic solvency and compliance of commercial and financial obligations that, according to this Act, may be disseminated, shall be permanently updated. The obligation to update such data is responsibility of the companies, people and entities which store, process and impart this information..."*

This article explains that modifications to personal data shall be made from the complaint made by the affected party or data subject to the data controller who is obligated to keep them updated.

The right to opposition is not expressly contemplated in the Act. It consists on the faculty of data subjects to address the person responsible for the public or private archives, records or data banks and request the cancellation of their data processing. It could be for the following reasons: when there is no consent (except for public sources), when the processing is carried out for advertising purposes and when the processing has the purpose of adopting a decision referred to the affected persons and based solely in an automated processing of their personal data. None of these aspects are contemplated in the Act or in their amendments.

Principle of Proactive Responsibility: Actions and Responsibility

The duty of keeping updated all files, registries in any of their forms of data processing destined to give reports, is under the responsibility of people in charge of data processing who can be: natural persons, companies or institutions which supply information.

Article 9 of the Act, in its final paragraph states that:

---

14 "Very personal" is said of the one so intimately consubstantiated with the person, that is not transmissible since it is not inherent (Montoya Melgar, 1995)

15 The Act had amendments in 2015, which complement art. 7 of act 1969/02. Since then, it is an obligation to update databases and to update the information of debtors on minimum wages which shall not be included to the Informconf list (debts less than 50 minimum wages, a little more than 3 million guaranies). It also had a rectification on provable information through any appropriate document, when the debt is settled, http://www.abc.com.py/nacionales/modifican-ley-de-informconf-1312696.html

"Companies or institutions which provide information on the patrimonial status, economic solvency and the compliance of commercial and financial commitments shall implement system procedures which automatically delete from their information system the non-publishable data, in accordance with the deadlines established in this article"

Principle of Limitation of the conservation period

The present Act establishes limitations in the time necessary for the purposes of the personal data processing, but it only limits its transmission and dissemination as expressed in art. 9 of Act 5543/2015 and the same article in Act 1969/02. Therefore companies, people or institutions which provide information about the patrimonial status, economic solvency or the compliance of commercial obligations may not transmit or disclose them. However, there is no mention about the elimination of the data after a certain period of time, this action may be carried out at the request of the data subject.

Penal Code

This legislation applicable in criminal matters contemplates punitive legal rules that protect privacy in the Paraguayan jurisdiction and which complements the safeguards the State must have for the protection of personal data in the country.

The Penal Code, Act N° 1160/97 typifies in chapter VII criminal offenses against the life and privacy of people. Among them, there are: article 141.- Violation of domicile, article 144.- Tort of the right to communication and to the image, article 146.- Violation of the secret of communication, and article 143.- Privacy tort. The latter refers directly to the public exposure of the person's privacy, sexual life, family life and health status.

The penal code is also used to sanction the non-compliance of companies and institutions that provide information on the patrimonial status, economic solvency and compliance of commercial and financial commitments. In addition, it is sometimes used to force companies to implement system procedures that eliminate automatically information of non-publishable data, according to Act 1682/01 and amendments.

Code of Judicial Organization

The Act 1682/01 amended by Act 1969/02, in its article 2 establishes that all information stated in public records are of free access, including Act 879 of the Code of Judicial Organization. Therefore, registries created by the latter are public and accessible "for those who have a justified interest in ascertaining the status of registered real properties or rights in rem" (art. 328 (National Congress, 1981)).

These registries of the judicial body reveal the patrimonial status, economic solvency and the compliance of the financial and commercial obligations of people. So, according to this code, these registries can be disclosed if data subjects give their consent in writing, except for the compliance of legal obligations of the public authority or justified in the public interest.

Act 642/95 of Telecommunications

This Act regulates all kinds of emissions and propagation of electromagnetic communication signals that are in the public domain of the State. In addition, it creates the regulatory body named National Commission of Telecommunications (CONATEL) which shall ensure compliance of the Act.

It includes aspects of data processing in the title IX Regime of subscribers and users protection:

Article 91.- It is the obligation of the owners of the exploitation of public telecommunication services to freely publish and distribute the guides and list of their respective users, in accordance with the

corresponding regulatory norms. The users shall be entitled to the non-inclusion of their names in such guides and list.

This Act implies that any licensee of the telecommunications domain frequencies, such as a Telephone Service Company, has the faculty to publish its registry of subscribed users through its telephone book. However, any data subject may oppose to the publication of their personal data.

Resolution 1350/2002 By which the Obligation to register the call detail record for a period of six (6) months is established

The Resolution 1350/2002 of CONATEL[16] contradicts the Act 642/95 of Telecommunications expressed in articles 89 and 90 on the inviolability of telecommunications correspondence and the Decree of the Executive Branch 14135/96 [17]. This Resolution gives power to the companies who operate telephone services to store the call detail records of all users in Paraguay for a period of six months:

> *Article 1.- To establish the period of six (6) months as a mandatory period to store all incoming and outgoing call detail records of all the lines which are part of the customers portfolio of the different operators of mobile phone service (STMC) and/or System of Personal Communication (PCS).*

Phone records, SMS and localization data of mobile devices are already stored for a period of 6 months through the Resolution of CONATEL of 2002, when several kidnappings for ransom took place that shocked Paraguayan society[18].

The pre-investigative measure for any type of offense not only reflects a disproportion in the aim pursued. And it obviously leaves aside the ideal of a minimal intervention through the punitive system of the State, what is called "minimal criminal law".[19]

Electronic Commerce Act and its regulatory decree

The purpose of Act 4868/2013 of Electronic Commerce is to regulate everything concerning commerce and contracting conducted through the Internet or equivalent technological means. In the first chapter on "Principle of free competition" a series of restrictions are contemplated which are considered invulnerable, among which are the protection of persons as consumers or users and the protection of personal data, personal or family privacy of the parties or third parties and the confidentiality of records and bank accounts (art. 6).

The law establishes minimum conditions for protection, such as the responsibilities of suppliers (Chapter III), notification of infringement of third party rights (art.18) and consumer or user rights (art. 30).

On the other hand, companies are obligated to store their users' metadata for a minimum of 6 months, according to article 10 of the Act 4868/2013[20] on Electronic Commerce. In order to

---

16 National Commission of Telecommunications (CONATEL), Resolution 1350/2002 By which the Obligation to register the call detail record for a period of six (6) months is established (National Commission of Telecommunications (CONATEL), n. d.)

17 By which regulatory rules are approved («Act Nº 642/95 "On Telecommunications"», n. d.)

18 "Última Hora" Kidnappings in Paraguay. Available at: http://www.ultimahora.com/los-casos-secuestros-paraguay-n460811.html [Consultation date: 5 January, 2017].

19 "Minimal criminal law means minimizing criminal circumstances and their general codification by decriminalizing all those conducts which do not offend fundamental properties and which saturate judicial work with a useless and harmless expense of the scarce and expensive resource which is the sentence and have the triple effect of the general weakening of the guarantees, the inefficiency of the judicial machinery and the devaluation of juridical properties worthy of criminal protection" Ferrajoli, Luigi. Crisis of the political system and jurisdiction: the nature of the Italian crisis and the role of the magistracy. Sentence and State Magazine, year 1, number 1-Argentina 1995: Publishers del Puerto s.r.l. p.113.

20 This legislation served as a precedent to draft the Act "Mandatory traffic data Conservation" which intended to force ISP to massively store communications metadata of all users for a period of 12 months

safeguard the constitutional right that we described as "informational self-determination", [21] it is imperative that ISP inform their users what personal information they are holding as well as the measures to safeguard their personal data against possible attacks or threats on such information.

Article 10 of said law establishes:

> *"Providers of Intermediation Services and Providers of Data Storage Services shall store the connection and traffic data generated by the communications established during the provision of a service, for a period of 6 (six) months, in the terms established in this article. For the compliance of this article's provisions, data shall be stored solely for the purpose of facilitating the location of the terminal equipment used by the user for the transmission of information.*
> *Providers of Data Storage Services shall store only those essential data to identify the origin of the data stored and the moment in which the service started.*
> *They shall not use the data stored for purposes other than those permitted by law, and they shall adopt proper security measures to avoid their loss or alteration and unauthorized access to them".*

On the other hand, the Act 4868/2013 of Electronic Commerce and its regulatory decree 1165/14 forces to inform and protect the users' data compulsively; in its article 9 it establishes:

> *"Obligation of the Providers of Intermediation Services. Providers of Intermediation Services consisting on the provision of services of Internet access shall be bound, notwithstanding the provisions in force on the Services of Internet Access and Data Transmission established by the Competent Authority, to: a) inform their customers in a permanent, easy, free and direct way about the different means of technical nature which increase the levels of security of the information and allow, among other things, the protection against computer viruses and spyware, and restriction of unwanted e-mails; b) inform about all the existing tools to filter and restrict access to unwanted Internet contents and services or those that may be harmful for children and adolescents; this obligation of information shall be accomplished if the corresponding provider includes the information required in its main Internet site. a) suspend access to a content or service when a competent body, in exercise of its legally attributed competences, requires that the provision of a service is interrupted or that a content is removed if it violates the provisions in article 6"*

In article 11 of the regulatory decree 1165/14, the following is stated:

> *"Duty to Inform and Data Protection. The provider of goods and services by electronic distance must inform the consumer or user the purpose and process that would be given to their personal data, in accordance with the current Act relating to the matter. Moreover, it shall inform the recipient of the data provided and the person in charge of guarding or storing the information provided. The provider of goods and services shall use secure systems to prevent the loss, alteration and access to unauthorized third parties to the data provided by the consumer or user".*

The guarantor Institution and the one in charge of monitoring the compliance of the Electronic Commerce Act is the Ministry of Industry and Commerce, which has to coordinate inspections and control the different Internet providers. It shall also apply sanctions for faults not specifically provided in the Consumer Protection Act and the ones established in the Electronic Commerce Act.

---

for "criminal investigation" purposes. The initiative was approved in the Chamber of Deputies at the end of 2014 but after a strong awareness campaign and rejection due to the risks implied, the Chamber of Senators rejected the proposal. The campaign was called "Pyrawebs" and is available at https://pyrawebs.tedic.org/

21 Informational self-determination complements in a positive way the right to privacy/intimacy, since it is not only about the impossibility of third parties to meddle in what happens in a person's life, but in the possibility people have to control the information concerning themselves and exclude it from the knowledge of others in advance or even once that information has been circulated.

General Act 861/96 of Banks, Financial and other credit institutions:

Chapter II of Act 861/96 of the Secrecy Duty, in its article 84 – Secrecy of Transactions – establishes:

> *"Institutions of the Financial System, as well as their directors, administrative and supervisory bodies and employees, are prohibited from providing any information on the transactions with their customers, unless they expressly authorize it or it involves the provisions of the following articles. The prohibition shall not reach the cases in which the disclosure of the amounts received from the different customers is bound for the purposes of liquidation of the banks or financial institutions"*

This and subsequent articles establish minimum rules on the publication and disclosure of personal information including administrative sanctions in case of non-compliance without prejudice of the criminal responsibilities established by the Acts.

Act 125/1991 That establishes the New Taxation Regime

Chapter VI on Duties of the administration, in article 190[22], expresses:

> *"Secrecy of actions: declarations, documents, information or complaints that the Administration receives and obtains shall be private and can only be used for the purposes of the Administration. Employees shall not, under penalty of dismissal and without prejudice of their personal, civil and/or criminal liability, disclose to third parties in any way the data contained in such. The same duty of secrecy shall weigh on those who, not belonging to the Tax Administration, perform for them works or automatic data processing or other mechanisms that involve the use of private material of the Tax Administration.*
>
> *The information in this article may only be provided to jurisdictional bodies that are aware of the tax procedure and their collection, tax frauds, common debits, child support and family or marital causes, when they understand that it is essential for the fulfillment of their purposes and are requested through substantiated resolution. On the information provided this way, the same secrecy and sanctions established in the second paragraph shall govern"*

The Institution responsible for processing tax collection data in Paraguay and the application of the Act is the Ministry of Finance. Access to the data collected by this Act can only be made through the data subjects or their legal representatives.

Resolution N° 77/16 of the Secretariat for Taxation – Ministry of Finance

Resolution N° 77/16 in force since February 2016 intends to improve the verification of taxpayers' information through technology, in order to avoid fraudulent transactions. This is part of the compliance of the strategic plan of the Secretariat for Taxation (SET). Some of these fraudulent transactions that are intended to be fought are the large number of tax evasions through RUC inscriptions without consent and which lead to the issuance of false invoices. According to media publications (ABC Color, 2017) between the years 2013 to 2016 about 100 of these cases were reported, which are currently under judicial process.

Likewise, official statements explain that the current record of biometric data is free of charge and that such updating is voluntary, according to provisions of art. 8 of Resolution 77/16. However, the "marangatu" system of the SET blocks access profiles to legal persons, forcing the update in the system to be done in person. Once the people are present, the compulsory registration of the biometric data of the legal representatives is carried out. This clearly contradicts the voluntary nature expressed in the official statement.

Regarding proportional measures and biometric data, the former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms, Martin Scheinin, determined

[22] Act on Taxation Regime (National Congress, 1991, p. 91).

in his report published in 2009 that the use of biometry may be legitimate for certain circumstances as terrorism cases, he is especially concerned about:

"the cases in which biometry is not stored in an identity document but in a centralized database, increasing the risks for the information security and leaving individuals vulnerable. As biometric information increases, error rates can increase significantly [...] Increase in error rates can lead to unlawful criminalization of individuals or to social exclusion"

On the other hand, the Rapporteur highlights a key element on the irrevocability on biometric data:

"*Once copied and/or fraudulently used by a malicious actor, it is not possible to issue to an individual a new biometric signature [identity]"*

Therefore, it is essential to think of a personal data protection Act which contemplates these technological advances and aims at limiting the possibilities of future abuses and that can be analyzed with rights perspective.

Access to Public Information Act

The right to information and the right to personal data protection are complementary rights that are defined in "sister" laws. A priori there is no real collision or conflict between both rights, however, the need for transparency must reconcile with the legal interest protected by laws, such as fundamental rights of people and, specially, with the right to privacy.

Access to information generated in the public administration is regulated by Act 5282/14, which is in force since April 2015 through its regulatory decree 4064/15. It is closely related to article 28 of the CN. Article 1 of the above mentioned Act states that its purpose is:

> *"[...] guarantee to all people the effective exercise of the right of access to public information, through the implementation of corresponding modalities, deadlines, exceptions and sanctions which promote the State transparency".*

In article 2, public information is defined and, at the same time, the exceptions are established: public information is the one "produced, obtained, under control or in power of public sources, regardless of their format, support, date of creation, origin, classification or processing, unless it is established as secret or of private nature by law"

Article 22 refers to the secret public information but without going in depth in its meaning by indicating some legislative rule. It is limited to defining it as "the one that has been or is qualified or determined as such expressly by law"

Likewise, institutions are obligated to follow the principle of active transparency, in accordance with regulation 4064/15 of the Act, through which they have to progressively publish in their official web sites "all public information in their possession, except the ones established by law as secret or of private nature" (art. 14).

It should be noted that the definition of secret information or of private nature is not available in the Acts, which could lead to ambiguities in the application of them. However, the limits of the Act are well established in its article 18 and in articles 34 and 35 of the regulation. Article 18 refers to public databases, and is explicit in prohibiting the data output or "...original records of the archives of public sources in which they are stored [...]". Article 34 of the regulation establishes the rejection mechanism of a request for public information, which should be based on "a legal norm with a hierarchy not inferior to that of the Act", as for example Act 1969/02 which regulates information of private nature. But article 35 of the regulation is the one that establishes the basis for the resolution

of controversies between the access to information and the protection of privacy or processing of personal data.

The criteria for a rejection to a request of public information is based on what is proposed by the Model Act on Access to Information of the OAS (Torres, s. f.). It effectively incorporates the test of public interest as the maximum guide for the application of exceptions. It affirms that the public source must substantiate a denial by showing that the information is indeed an exception, taking into account:

> *"a) that the exception is legitimate and strictly necessary in a democratic society based on the standards and jurisprudence of the Inter-American system of protection of human rights;*
>
> *b) that the disclosure of the information may cause a substantial damage to an interest protected by law; and*
>
> *c) that the probability and degree of such damage is greater than the public interest in the disclosure of the information" (art. 35)*

Article 36 offers another way of solution in case of tension between the right to access to information and the protection of privacy or personal data processing. In line with the Model Act of the OAS, to comply with the standards of the Inter-American system on the regime of exceptions, it establishes the principle of "in dubio pro acceso". That is, in words of the regulation:

> *"in case of reasonable doubt on whether the requested information is protected by the principle of publicity or if it is reached by a causal of exception, it must opt for the publicity of the information"*

Finally, article 37 promotes the partial disclosure of the information in case a document contains information that must be published and information that is causal of exception. In that case, information that may be known should be disclosed.

The body of the application of the Act are the Offices of Access to Information, in accordance with article 10 of the regulation that shall be created by every public sector body and are depended upon its highest authority. Denials of access to public information shall be dictated by this authority.

The Act "That prohibits unauthorized advertising by the users of mobile phones"

The present Act[23] was approved in the Congress in May 2017, it is currently in the stage of promulgation by the Executive Branch, and therefore, at the closing of this research, there is still no number nor validity of the Act.

According to the drafters of the Act, this anti-spam law is inspired in the Argentinian regulation colloquially called "Don't call me"[24], which establishes a list of people who do not want to receive unauthorized advertising. In Paraguay, such list shall be managed by the Secretariat for Consumer and User Protection (SEDECO). In case this request is ignored and the person receives unwanted advertising, the person can legally sue the sender of the message (art. 6).

However, this new Act does not solve the fundamental problem, since it lacks a comprehensive approach for the processing of personal data. A problem so complex as that of personal data nowadays cannot be addressed with regulations that simply prohibit spam, but do not take actions against the uncontrolled sale of personal databases and that leave people helpless in case of possible abuses. The protection of personal data must be faced with a rights approach, applying as a

---

[23] Legislative Information System (SILPY) Status of the law http://sil2py.senado.gov.py/formulario/FichaTecnicaExpediente.pmf?q=FichaTecnicaExpediente%2F107665

[24] The Chamber of Deputies approves the Act against unwanted messages. Date: 6 December 2016 http://www.ultimahora.com/diputados-aprueba-ley-contra-mensajes-molestos-n1045679.html

cornerstone the structure of the personal data protection system, which are: consent and informational self-determination.

On the other hand, it was not taken into account the Act 4868/13 of Electronic Commerce on the regulation of unauthorized advertising, which is in force and has a specific section about unwanted advertising in its articles 20 to 23. It establishes that in case the providers of goods and services want to send unwanted communications, they must expressly indicate that such communication was not requested; include simple ways for the user to exit the recipients' list; and also indicate that they have not infringed the privacy rights (art. 23), by seeking a balance between "*prohibition against unauthorized sending*" and "*commerce*".

Regarding the anti-spam Act, the consent must be prior to the "*Don't call me*" list. The same shall apply to the processing of personal data from the same collection. The person shall consent in a previous, express, free and informed manner about the processing of their data, at the time of the collection, that is, the purpose for which they are collected and stored, regardless of whether they are or not in a "*Don't call me*" list.

This debate shall also address problems that may lead to a transfer of personal data, if they are collected or used outside the competence of the public or private sector.

National and International Jurisprudence

The following paragraphs are a series of cases, both nationally and internationally, that set precedents on how to apply the regulations regarding the subject under study; this is what is known as jurisprudence and can be very useful for the drafting of the new legislation in the matter, as well as for future legal cases.

IACHR: Case of Escher et al. v. Brazil

The Inter-American Court of Human Rights (IACHR) on the contentious case in which Brazil was convicted (IACHR, 2009) for the unlawful telephone interception and monitoring of telephone lines in a criminal procedure. The Court pointed out that the right to privacy protects both the contents of the electronic communication and other data specific to the technical process of the communication. These include the metadata or traffic data, understood as "the destination of outgoing calls or the origin of incoming calls, the identity of the interlocutors, frequency, time and duration of the calls, aspects that can be verified without the need to register the content of the call through the recording of conversations".

This jurisprudence is binding on our national jurisdiction since Paraguay recognizes the Court as an International instance for human rights. In addition, article 31.1 of the Vienna Convention (OAS, 1961) provides that if a State signs an International treaty -particularly in the field of human rights- it has the obligation to make its best efforts to implement the pronouncements of the corresponding supranational bodies (Fuenzalida Bascuñán, 2015).

Therefore, this IACHR sentence must be taken into account for the compliance of the protection of Human Rights. On the other hand, it implies compliance with the treaties and directives of San Jose which impose the international responsibility of the State in any of its three branches. (art. 1.1 and 2 of the Pact of San Jose).

Sentence of the Supreme Court N°674/10, The Case of Cecilia Cubas

The sentence of the Supreme Court of the Judicial Branch N° 674/10[25] on the extraordinary appeal of cassation requested by the defendants of the kidnapping and murder of Cecilia Cubas, was declared *inadmissible*. This emblematic case involved the daughter of the former President of the Republic, Raul Cubas Grau (August 1998-March 1999) who was kidnapped on 21 September 2004, after a group of criminals surrounded her vehicle a few meters from her home near the capital of Asuncion. Cubas was found dead on 16 February 2005 (ABC Color, n.d.).

The Supreme Court stated that all procedural guarantees were complied and that there was no violation of communications by the Public Prosecutor's Office by requesting, without a warrant, the metadata of the phone calls made by the suspected perpetrators of the kidnap.

> *"The answer given by the Court of Appeal was express and satisfactory. In accordance with article 228 of the CPP, the Public Prosecutor's Office may request reports to any person or public or private sector body. Article 316 of the CPP, within the faculties of the Public Prosecutor's Office, reaffirms that "it may require information to any civil servant or employee, depending on the circumstances of the case. All public authorities are obliged to cooperate with the investigation, according to their respective competencies and to comply with requests for reports that are made in accordance with the law".* [26]

In addition, the Public Prosecutor's Office accessed the reports and then processed them without it implying any violation, either of a constitutional or legal order. As it was illustrated, the information provided facilitated access to the data of the owners of the line, date, time, hour, number of incoming and outgoing calls and the specific geographical location where they were made. The access was to the detail of all the calls and not to the content of them. In case the contents had been accessed, the *inviolability of the communication* and the *right to privacy* would have been violated.

To summarize, the analysis of the Supreme Court on the inviolability of communication and access to personal data is[27]:

- The provisions of article 36 of the Republic's Constitution on the right to the inviolability of documentary heritage and private communication, protects the communication itself: the words that could have been said by the accused parties in this process through a phone. Not so the consequent of these communications, which was the object of work by the legal expert.
- Expert test on interference on a telephone line: in the expert's report about interference on telephone lines, it is concluded that the data mentioned are the notes taken by the telephone company consisting on the phone number investigated, outgoing and incoming calls from that number as well as the time of the calls; none of these make the telephone communication which consists on the message a person says and the other one listens through a telephone device.
- Testing of legal experts: in the legal expert's report on the interference of telephone lines, work is done on the data that are stored on the telephone calls after a communication, and not on the communications that generated the data. The CN protects communication but no the interference of telephone lines which were the object of the expert's report.
- In the expert's report on the interference of telephone lines, since the communication itself was not the object of the expert's report but the information provided by such communication, the warrant was not mandatory since the expert's report did not affect the scope of the constitutional protection.
- In the expert's report on the interference of telephone lines, the telephonic communication was not examined, it is not known with certainty what could have been said by the people who owned the investigated numbers. It is concluded that it was not intercepted since there is no

[25] Agreement and Sentence Nº 674/10 "Extraordinary Appeal of Cassation interposed by the Public Defender Sandra Rodriguez Samudio in the lawsuit Anastacio Mieres Burgos and Others on Kidnapping and Others". File. N° 773, Folio 245

[26] Supreme Court of Justice. Courtroom: Penal Subject. Inviolability of Private Communicartion. Evidence. Means of Evidence. Test of legal experts. Interference of telephone lines. Agreement and Sentence N° 711 of 20/08/14.

[27] Based on the analysis (Jorge Rolón Luna, Maricarmen Sequera Buzarquis, 2016)

third party who had been listening to such communication with the proper technology for it. Therefore, it was not possible to record it or reproduce it.

It is worrying that the Court has taken these considerations without evaluating the international criteria that shall be applied on the topic of metadata. By analyzing from the perspective of the application of the Human Rights on Communication Surveillance, it is considered that the Public Prosecutor's Office does not have the attribution to require reports of such characteristics, since it violates privacy and personal data, even more if they have been requested without a warrant.

Ricardo Canese vs. Paraguay (Funds, Reparations and Court Fees)

Inter-American Court of Human Rights Case Ricardo Canese Vs. Paraguay, Sentence 31 August 2004 (Funds, Reparations and Court Fees). The present case refers to the international responsibility of the State for the conviction in a process of defamation and slander, and the restrictions to leave the country imposed in detrimental to Ricardo Nicolas Canese Krivoshein.

The facts of the present case started in August 1992 during the debate on the electoral dispute for the Presidential elections in Paraguay. Mr. Ricardo Canese, who was a presidential candidate, testified against Juan Carlos Wasmosy, also a candidate, for alleged illegal actions when he was president of a consortium. On 23 October 1992, the directors of that consortium filed a criminal complaint before the Criminal Court of First Instance against Mr. Ricardo Canese for the crimes of defamation and slander. On 22 March 1994, he was convicted in the first instance, and on 4 November 1997 he was convicted in second instance to two months of imprisonment and a fine of 2.909.000 guaranies. As a result of the criminal procedures against him, Mr. Canese was subjected to a permanent restriction to leave the country. On 11 December 2002, the Criminal Division of the Supreme Court of Justice in Paraguay annulled the convictions against Mr. Canese, issued in 1994 and 1997.

It is important to mention that this litigation is transcendental to reaffirm the right to access to public information and the limits of protection of personal data for the public interest. The sentence emphasizes the need for citizens to know the information of the candidates for public posts in order for them to make the right decision when it comes to voting in the national elections, without restrictions and thus respecting the freedom of expression as an essential tool for the formation of public opinion.

International Instances

The agenda on the protection of personal data has been under discussion for a very long time in International instances. Paraguay is part of several working groups, with the commitment to adapt Act 1682/2001 to the standards of the Directive of the European Union and the new scenario of digital economy.

Common Market of the South

The constitution of the Common Market of the South (MERCOSUR) seeks the free movement of people, goods and capital and was made through the Treaty of Asuncion. The quality of this body, which seeks to regulate the transfer of data to other countries in areas such as human resources, financial services, e-commerce and education, that are part of the global digital economy, entails the protection of the fundamental rights of citizens by adapting the legal instruments to the process of technological, economic, social and cultural innovation.

Within this framework, the initiative of MERCOSUR Digital was created for the data processing between MERCOSUR and the European Union; currently, this process is without much progress (MERCOSUR, 2008).

Organization of American States

The Department of International Law under the Secretariat for Legal Affairs (SAJ) of the OAS, is currently leading the work of the Data Protection Network (RID).

Our country is an observer of the network through the Secretariat for Civil Service[28]. One of its objectives is the creation of an "Inter-American modern Act on personal data Protection"[29]. In addition to participating as observers of the European Supervisor of Personal Data Protection on behalf of the European Union, among other international organizations.

To this is added the *Proposal of Declaration of Privacy Principles and Personal Data Protection in the Americas*, adopted in 2012 by the Inter-American Legal Committee of the Organization of American States (OAS)[30]. However, this proposal does not establish high lines of protection, falling below the standards of the Directive of the European Union and other countries which are in line with European standards originally foreseen by the previous Directive 95/46/CE.

Ibero-American Data Protection Network (RIDP)

This network is based on the agreement reached at the Ibero-American Meeting of Data Protection (EIPD) between representatives of 14 Ibero-American countries, held in La Antigua, Guatemala, from 1 to 6 June 2003.

It is a working group composed of countries of Latin America and Spain, from the public and private sector. In our country, it is composed by the Public Ministry, Judicial Branch, the Paraguayan Association of Digital Law and the Ministry of Industry and Commerce[31].

This June 2017 was the official launch of a document of "Standards for protection of personal data for Ibero-American States" (Ibero-American Data Protection Network, n.d.). The document seeks to assemble with international forums with the level and imminence of the subject.

Organization for Economic Cooperation and Development

Paraguay is officially part of the OECD since 2017[32]. This organization has recommendations that constitute documents to guide its Member States. In this line, there is an agenda of data protection with the purpose of establishing basic regulations of data protection which guarantee the free flow of information as well as to avoid regulations that create protectionist barriers in international trade. The OECD issued guides on International Circulation of Personal Data for the Protection of Privacy and Security of Information Systems[33].

United Nations

There are UN guidelines for the regulation of computerized personal data files through its resolution 45/95 of the General Assembly of 14 December 1990 "*Guidelines concerning Computerized Personal Data Files adopted by resolution of the General Assembly of the United Nations"* (UN, 1995). It addresses basic protection issues which must be followed as a guide for internal standards. It is updated and

---

28 Observers accredited to the RIPD http://www.redipd.es/la_red/Miembros/index-ides-idphp.php

29 Documentation they have formed and will be part of the process of preparation, discussion and approval of the Inter-American modern law on the Protection of personal data of the OAS available at http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp

30 http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

31 Members of the Ibero-American – Paraguay Network: http://www.redipd.es/paises/paraguay-ides-idphp.php

32 Paraguay is already part of the OECD member countries http://www.lanacion.com.py/2017/01/26/paraguay-ya-forma-parte-los-paises-miembros-la-ocde

33 "Guidelines on the "Protection of Privacy and Transborder Flows of Personal Data" of the OECD («2013 OECD Privacy Guidelines - OECD», n. d.)

complemented with the Resolution on *Privacy in the Digital Age* adopted by the UN General Assembly in 2016 (UN, 2016).

Analysis of Interviews

Personal data in databases of public sector bodies

In order to have a better idea of how databases are managed in practice, interviews were carried out to civil servants who have direct responsibility on the processing of such databases, and also to qualified experts. These interviews sought to find out whether or not these public sector bodies have incorporated principles and practices of personal data protection contained in their databases. This chapter summarizes the main findings which are organized under the categories associated to the protection standards outlined in David Banisar's work and stipulated in the new Regulation of the European Union (EU) 2016/679.

The following paragraphs describe the nature of databases –which databases are under the responsibility of the public sector bodies, what personal data they contain-, how protection principles are applied or not –collection, notification, purpose, limitation of use, etc.- and comments are added about other findings that emerged during the interviews.

Nature of Databases

All public sector bodies interviewed have databases that contain personal data. These data are related to the implementation of educational, housing, customs, commercial, fiscal and social assistance policies. Most of them are digitalized, although there were some cases that still contain personal data in physical format.

Among these bodies, databases coincide with some personal data such as name, surname, date and place of birth, ID number, address and e-mail. They differ according to the activities they perform. For example, for the implementation of housing policies, the databases contain information about people's income, employment status and filing data. That is, they have information on whether people have children or not, if they are in charge of older adults, etc.

Through the interviews, personal data are identified in the following sector bodies:

Databases	Personal data	Purpose of creation	Act of Establishment of the Body	Public Sector Body
Unique Taxpayer Registry (RUC)	Name and surname, e-mail, address, economic activities, employment, RUC (Unique Taxpayer Registry), affidavits, payments made.	Tax management[34]	Act 125/91[35] which establishes the new tax regime and its amendments	Sub-Secretariat of State for Taxation of the Ministry of Finance

34 Interview with an employee from the Sub-Secretariat of State for Taxation

35 Available at: http://www.impuestospy.com/Leyes/Ley%20125_91_art1_25.php

Databases	Personal data	Purpose of creation	Act of Establishment of the Body	Public Sector Body
Unique Student Registry (RUE)	Name and surname, date and place of birth, ID number, data of father, mother or legal guardian, academic record of middle school students, educational institution	Record of students of the Paraguayan educat ional system[36]	Resolution N° 8655[37] by which it is authorized the implementation of the unique student registry in the educational institutions of all levels and modalities of official, private and privately financed management of this Ministry	Ministry of Education and Science
Data registered for the application of the housing plan of the institution	Name and surname, place of residence, economic activities, employment status, economic capacity (income), number of children, children's health status, seniors in charge	Application of the housing plan of the institution; evaluation of beneficiaries[38]	Act 3909[39] which creates the National Secretariat for Housing and Habitat "Senavitat"	National Secretariat for Housing and Habitat
Data registered for the activities of international trade of the institution	Name and surname, ID number, RUC, address, phone number, e-mail	The data are used for the management of the operating and administrative areas of the entity such as, for example, summary declaration, detailed declaration, tax collection, bank guarantees and insurances for customs operations, among others[40]	Act 2422[41] Custom Code	National Customs Office
Data registered for the social programs provided by the institution	Name and surname, ID number, address, salary, number of people living in the house	Evaluate the "poverty level" of the family to grant social benefits or not	Act 1602/01[42] and operating procedures manual of the institution	Secretariat for Social Action

36 Interview with MEC employee
37 https://mec.gov.py/cms_v4/documentos/ver_documento/?titulo=8655-2016-LAFUENTE
38 Interview with SENAVITAT employee
39 https://www.senavitat.gov.py/blog/leyes/ley-no-3-909
40 Answers sent by e-mail from a Customs Office employee
41 Available at: http://www.aduana.gov.py/uploads/archivos/codigo%20aduanero.pdf

Databases	Personal data	Purpose of creation	Act of Establishment of the Body	Public Sector Body
Clinical data of patients	Name and surname, address, health status, consultation history (very fragmented), hospitalizations	Have a health record of the population	Act 1602/01	Ministry of Public Health and Social Welfare
Social program of the institution	Name and surname, address, salary, number of people living in the house	Evaluate the "poverty level" of the family to grant social benefits or not	A decree and a protocol that authorizes the program to do the collection	Secretariat for Technical Planning
Academic data of students Teacher's work data Data for the management of Internet domains	Name and surname, ID number, registrations, grades, salary, e-mail	Manage the academic system, the payment system and the system of domain names of the National University of Asuncion	Establishment of the CNC	National Computing Center
Exports data Companies data	Name and surname, address, importer, income	Operate on imports and exports Generate a record of companies	Act 1602/01	Ministry of Industry and Commerce

Examples of databases

There are some emblematic databases such as the Unique Student Registry (RUE) and the Unique Taxpayer Registry (RUC). The first database is an information system that identifies all students of the Paraguayan educational system in charge of the Ministry of Education and Science. It was developed with the support of two international organizations, - the Organization of Ibero-American States and the Program for Democracy and Governance of the United States Agency for International Development (USAID) through the Center of Environmental and Social Studies (CEAMSO). In the launch of the tool, the Minister Enrique Riera, during his speech, referred to the tool as a "gigantic database in a single platform". The Vice Minister of Education, Maria del Carmen Gimenez, added that the system generates a "student ID, a student identity which will allow teachers, families and the Paraguayan State to manage all initiatives and resources with greater precision" [43] (OEI, 2016).

Specifically, the RUE contains data of all students and also of their guardians (father, mother, legal guardian). It also incorporates data of foreign students who attend an educational center in Paraguay. Thus, it said in one of the interviews[44]:

> *"The RUE (Unique Student Registry) is (the database) more sensitive since it collects information from minors. Data such as name and surname, date and place of birth, ID number –all identification data. Additionally, we keep information of foreign students, that is, there are students who do not have a Paraguayan ID and yet are educated here. Structurally they are the same information. We also have*

42 Available at: http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=1760
43 Available at: http://www.oei.org.py/index.php/presentacion-del-registro-unico-del-estudiante-rue/
44 Interview with MEC employee

contact information, data of father, mother, legal guardian, contact information of them, place of birth, to which institution they correspond, that is, where they are enrolled and all associated information [...]Regarding academic management of Nautilus, since 2012 we already have the academic history, but only of the students of middle school".

For its part, the RUC, according to the Ministry of Finance, which is responsible for the implementation of the fiscal policy of the country, is "*the ID number –personal and non-transferable- of all national and foreign persons, and of all legal persons (companies, service providers, industries, etc.) that carry out economic activities*" (Ministry of Finance, 2017). It explains that non-profit entities must also have RUC[45]. In an interview, the following was stated[46]:

"It contains all the main data of the taxpayer: economic activities carried out, employment, address, e-mail [...] Since its registration, all the traceability of the processes that govern the National Tax System are within that application. Type of taxpayer, presentations, affidavits, payments made, it has a checking account of the taxpayer [...]".

The management of these databases and the ones managed in other institutions explored in this research are analyzed under the principles of protection listed below.

Principle of collection

On this principle, the existence of legal frameworks which regulate the data collection are investigated, as well as the due notification to people when their data are collected. All interviewees refer to regulations which guide or regulate the data collection in their institutions. These regulations are varied and, in general, none of them refer exclusively to the processing of the data collected. Some interviewees mention the decrees of establishment of the institutions, as in the case of Senavitat and Customs Office. Other interviewees name ministerial resolutions which establish the creation of specific databases, such as the Unique Student Registry in the Ministry of Education and Science, and which indicate procedures and organizational charts that outline the management of such databases. They also refer to two Acts approved in recent years as legal frameworks that affect their work: Act 5282/2014 of free citizen access to public information (National Congress, 2014) and Act 5189/2014 which establishes the obligation to provide information on the use of public resources on remunerations and other rewards assigned to civil servants.

"[In the Ministry of Education] ministerial resolutions where, for example, the Unique Student Registry is implemented, and then whatever has to do with human resources"

"[In the Secretariat for Technical Planning] I have internal regulations that were approved by the legal advisory team, which I assume that took into account the national and international [regulations]. We also had a brief talk (with an expert in digital rights), who gave us some tips about things we cannot do as a government. It was also considered at the time of making the operational procedures manual, which includes how to protect personal data"

We found that technicians and people in charge of processing or guarding the databases had an insufficient level of knowledge on protection regulations. To justify this ignorance, the interviewee of the CNC appeals to his role of computer technician:

"the thing is that we are only technicians [...] More than that, we do not have... There is no regulation".

In other cases, they accept the current situation of lack of clarity regarding the regulations, without hesitations, as emerges in the interview with the SAS employee:

45 Available at: https://www.hacienda.gov.py/web-hacienda/index.php?c=77
46 Interview with the employee of the Sub-Secretariat of State for Taxation

> *"We are governed a little by that «institutional norm», which is not written, I am not going to lie to you. It is kind of the vision of the highest authority in saying: «this can be given, this cannot», and also the customer's face".*

On the other hand, as it was mentioned before, some of the interviewees explained that the data collection is supported by "*the establishment act*" of the body or by internal regulations, and it is probable that in such regulations there is no specification on the management of personal data[47]. One of them said:

> *"The Act of establishment of Senavitat is what governs the scope of action of the institution. But there are no specific points as to the details of information, the protection... [...] Of course, it is not as explicit as that of the Treasury's Advocacy, Taxation..."*

A Customs Office employee reinforces the idea of support by internal regulations:

> *"The Customs Code in article 8 where it authorizes the use of information technologies and automation [...] in articles 17, 18, 19, 20, 31, 34, 36 and 40 where it defines the action, rights, obligations and disciplinary regime of people related to the activity [...]"*

As it can be observed, the interviewee talks about action, rights and obligations, but does not refer to matters inherent to the processing of personal data.

Meanwhile, the MEC interviewee talks about an internal policy of information management:

> *"We have a policy of information management, we have implemented some procedures, and there are ministerial resolutions which regulate the implementation of systems and, consequently, the roles of each of the actors".*

Again, some bodies have made further progress by creating their specific regulations on personal data, while others are based on outdated regulations and others in "unwritten regulations". One of the interviewees claims to know the current law on "Private information" (National Congress, 2001):

> "[In the MSPBS] I think it is the «private information» and sensitive I don't know any other law. Because: the health issue is private and sensitive. Any type of information which indicates, individualizes or allows to individualize..."

In the interview with the MIC employee, the Act of private information is also mentioned:

> *"There is an Act that governs personal data. Some data are confidential and some are public. For us, for example, the importer is confidential data, for example: who are they selling to? That is information that we cannot publish because the competition can use it to get advantage. Certain data such as income and others, we cannot, because they are confidential. But then the rest of the data are all related to the country balance of payments and are public data. We do not have many confidential data".*

There is a certain tension or a diffuse line that arises in the theoretical framework of this research on the access to public information and personal data protection. The interviewee of the SAS put it this way:

> *"I don't remember the Act, but part of this Act is the one that we as civil servants, there is an Act of transparency that was made in 2015".*

We shall remember that transparency and access to public information can collide with the processing of personal data and the thresholds must be clearly marked. Since there is no organic Act of Data Protection, these thresholds are currently established by each public sector body.

---

47 The possibility of knowing the internal regulations of each public sector body escapes the scope of this research

It is true that this is the right area to deal with legal issues, but there is also a widespread lack of knowledge, which can be understood because of the fragmented regulatory framework and the lack of an Organic Act on Personal Data, as well as an independent comptroller body which grants greater guarantees of protection. Thus, one of the qualified informants said:

> *"With telephonic data, the first line of defense of all of us should be CONATEL. But apart from that, since we do not have an organic Act of data protection that should be the one that is above all that, then we are actually orphans"*

Finally, there are national Acts that apply to a determined body, as it comes up in the interview with the SET employee:

> *"Act 125/91 basically comes off in a lot of rules and actually always, when we speak in that sense, we say: Act 125 and its amendments. From there, a lot of rules emerge. And really all existing rules apply to us".*

As it can be seen from all the interviews, the situation is confusing. In the first part of the analysis of the findings, a legal analysis is presented covering the current national and international legislation and the binding jurisprudence, which reveals the status of the regulatory framework concerning the collection and processing of Personal Data and also shows the existence of important legal loopholes. In the words of the CNC interviewee:

> *"We usually have big philosophical discussions about what is publishable and what is not. That is precisely because we do not have a well-established regulatory framework which tells you where and how far. One interprets that the ID number is public, others interpret that the name, both [...] We need lawyers to study the technology-related issues, there are very few lawyers who are specialists in that".*

Regarding the **notification,** most interviewees claim that they let people know when their data are being collected and for what purposes. However, it is not clear whether institutions make this notification by principle of personal data protection or to satisfy a need for identification of beneficiaries.

For example, in order for people to be able to access the benefits of the social programs, they have to provide their personal data in documents that have the nature of affidavits.

> *"It is previously notified. We have field employees. In the countryside there are about one thousand people who closely accompany the families and they know when they will go to intervene a certain district, through the Municipality. The form, currently a parallel document is signed, since I told you, it is done with tablets, but there are places where it is still done in paper; the head of the family signing at the bottom, as an affidavit. This is what it was done, they read it and if they are sure of all the data that is there, they authorize us to take that data and record it" (on the notification of data collection in the SAS).*

> *"We ask: Do you want to be a part of this survey and give your data to be a potential beneficiary of the following social programs?" (on the notification of data collection in the STP).*

Principle of purpose specification

On this principle, it is sought to identify the reasons why public sector bodies collect information. Some interviewees relate the data collection to the need to meet the objectives and activities of the institutions where they work. However, there are no specific rules or regulations that outline the purpose of the collection of personal data.

> *"[In Customs] the data are used for the management of the different operating and administrative areas of the entity such as: summary declaration, detailed declaration, tax collection, bank guarantees and insurances for customs operations, among others".*

"[In the SAS it is collected] specifically for two reasons: one is the monitoring of families and the other one is the payment itself. They receive a payment, a fee, which consists of 72 installments. And for me to know how much I have to pay these people, I have to analyze it electronically. In total there are thousands".

Principle of limitation in use

On this principle, it is sought to know if the data collected are used with other purposes beyond the primary purpose of the collection. Some interviewees claim that the data contained in the databases are not used for purposes other than the ones they were collected for. However, since there are no specific regulatory frameworks for the purposes of data collection, there are doubts concerning the full compliance of this principle. Only one interviewee specifies that the data collected is limited to the use stipulated in the establishment regulation of the institution. Others, however, indicate that the data are used for statistical purposes or are shared with other public sector bodies.

"[In STP] that information has not been used in any way for anything other than helping them. It has been shared with people in charge of planning social programs, for example, which is explicitly the purpose for which they were collected" (on the use of personal data collected for social programs).

"The data registered of people linked to the customs activity are used for the purposes foreseen in the Customs Code. They are not disclosed or shared beyond the original purpose of their collection".

"[In the SAS] the programs are the ones that have the most data, and each one has its own database. At the same time (...) we use them to take statistical analysis, among other things".

Principle of data quality

The principle of data **quality** specifies that they have to be used for the same purpose they were collected for, and they have to be exact and updated. In addition, data that are inaccurate with respect to the purposes of the processing should be deleted.

Many of the interviewees agree that their institutions have mechanisms for updating the data, both in case they are erroneous, and over time, since the data must be adjusted to the reality of the data subjects. In the interview with STP it was mentioned that data subjects themselves have the possibility to update their information:

"The taxpayer itself has the possibility to update. In fact, not long ago, we made some changes [...] so that the data update becomes an obligation [...] What we enabled there is the possibility to do it through the Internet: most updates are being carried out through the Internet".

There are also testimonies such as the following, in the interview with the MEC employee, where parents update their children's data:

"The father himself can do it, within the registry [...] the father can access his child's data, which is his population. If he can access his child's data, then he can obviously modify them".

While in other cases, the institutions are the ones that systematically update data through procedures and protocols:

"[In the MSPBS] I understand there is an entire approved protocol for that. Not everybody can decide whether a data is wrong or not, and there is traceability in all the changes that are made".

There is a case where the institution that processes the data is not the same as the one that collects them. In this situation, a quality control is performed:

"All the CENSUS collection was not made by us: a big part of it was carried out with the DG [DGEEC] [...] So the quality was not that good in some cases. So the update also includes the correction of names, IDs, etc."

We can say that most of the institutions we are investigating comply with the principle of data quality in terms of purpose and update.

Principle of conservation

Concerning the principle of **conservation,** it refers to the period by which personal data are stored. We notice that the vast majority of public sector bodies do not have established time limits for the conservation of data. They lack protocols, mechanism or regulations for the destruction of personal data.

In most cases, this is justified by administrative or audit needs. The interviewee of SAS affirms:

> *"So that is why we don't delete them; for us is also an historical data [...] If we had a control, of the Audit Office, or some digital audit related to these families, for every payment that was made, even if it is not active"*

Another example in which the reason for not deleting the data is explained, arises in the interview with MEC:

> *"[...] that boy that started kindergarten, the information is only entered once, and when he graduates as an engineer he will have the same information. Today we talk of basically 20, 25 years. So, we don't plan to delete data. In fact, on the contrary, we have support mechanisms, we aim for high availability, rather than to delete"*

There was a case in which the interviewee stated that the procedures and rules for destruction are established, but they are not complied:

> *"There is a period for storage and a period for destruction, but it has to be done under legal procedures: but it is never done. They are stored, they are kept in a deposit «for ever», until they catch fire or something. It is very complicated to destroy a story, the procedure of destruction is not usually done".*

As it can be observed, being the public administration, most databases and data collected have to do with the granting of social benefits, administrative procedures o relationship between State and citizens. So, for control reasons, if there is no double benefit or similar justifications, such collection is justified.

Beyond these justifications, the periods for each case must be established. It is clear that ID data should not be deleted, while criminal records must be deleted 3 years after the corresponding penalty has been served. What emerges from the interviews is that State institutions are not noticing this principle of conservation.

Principle of Safety

On the issue of **access and transfer** of databases, most interviewees said that institutions manage strict criteria on access and transfers. All of them have strict data access policies with established roles and register of access. For example, in the interview with CNC the following was affirmed:

> *"You can have access to databases that are of administration or salary. But the levels are well defined and there is an audit for each access; and users are individualized".*

In another case, in the interview with SAS, the following is stated:

> *"Each program has a database administrator, and of course the ICT address in this case [...] In the department there is another administrator that is me, and there is a department from ICT, which is the development one, where another person also has access. There are three like that and that's it".*

In the interview with Senavitat, they said that the subject is still under a definition process:

> *"The roles are defined: we have a database administrator, we have people in the development area and operative people. It is all managed by profiles that define the access levels to the information or data. And we are also working on defining who are the ones that will authorize or unauthorize access".*

In one of the cases, a confidentiality agreement is made explicit with the civil servants in order to have a legal support in the personal data protection, as it appears in the interview with MEC:

> *"We make them sign a confidentiality agreement, including the entire technical team. Nobody can access the production servers. They can only access to test data, more or less we try to control the environment and the levels of access according to the function that each one fulfills".*

In terms of access, there is evidence of a consensus and the adoption of certain "good practices" which have to do with compartmentalization, levels of access and registration of access, in order to ensure that there are no wrongful access to data or, in case there is, to be able to make a corresponding analysis for the identification of the fault.

It is noteworthy that only one of the interviewees referred to the *Standard Model of Internal Control for Public Entities in Paraguay (MECIP)* which is a permanent control tool for the management in public sector bodies. As we mentioned, only the interviewee of the STP cited it as a regulation and source of good practices:

> *"We actually have a risks map that the MECIP requires us [...] For every action you make, you need to have a risks map. So, for example, if you have an action which is "grant access to a database", you have to put your risk map to it".*

On the other hand, concerning **transfers**, we found that practically no **international transfers** are made, and in one case there is the possibility of transfer but in a very aggregated and anonymized way.

In terms of **national and inter-institutional transfer**, there are several ways of exchanging data and information between public sector bodies: there are more precarious and insecure forms such as the sending through removable devices like compact discs, but there are also systematic and interconnected ways of doing the exchanges.

One example is the Integrated Information System of SENATICS (SII), in which public sector bodies make available to their peers several relevant data set which allow to accelerate certain processes and try to reduce errors. That is what the MEC interviewee explains:

> *"I don't know if you have already heard about the information exchange system between public sector bodies which is managed by SENATICs. It is a communication channel between public institutions in which they can make their data available in order for them to be used among all institutions. One example: the Identifications Department make their database available and we "consume" that information through a service, in that case we are being consumers. There is also the possibility of being provider of information and we are now proving the academic degree, for example".*

In the interview with SENAVITAT, one of the benefits of this form of sharing appears:

> *"[...] Today, those errors are trying to be minimized by accessing information from other institutions through the Integrated Information System of SENATICs".*

But there are also certain limits in the interview with SAS:

> *"But when I want to know about somebody, they ask me about the ID number and date of birth: that is not useful for me, what is useful for me is the complete database to be able to do the data crossing. The cross-references made are permanent, are big [...]".*

On the other hand, there is the Integrated System of Social Information (SIIS) managed by the STP and that contains information on beneficiaries of the different social programs of the government:

> *"They are institutions of the program «sowing opportunities» which have access to the «presidential control panel», that is, to the institutions that work in the social area. The access is controlled by a system, [...] systematized and controlled and also has a system auditing".*

In the interview with SAS, on the same system, it is affirmed that:

> *"There are different institutions which have social programs. What they are looking for is that people are not accessing to more than one social program, of the same person or the same family group".*

Moreover, it is specified that:

> *"This system that they have is a system of social integrated information, the vision of the previous government, which is that I write «Luis» and your ID number, and I know where you are: in which institution you are benefited".*

The Ministry of Finance manages an exchange system of tax information, called SIARE,

> *"In fact, the issue of salary is charged every month [...] then, when it's loaded, it is transferred to the integrated system SIARE, so that the Ministry can pay" 46.*

As it can be seen, there are many forms of exchange but there is an interesting tendency to do it in a systematic and centralized way, in order not to duplicate information and in order for databases not to proliferate in the different institutions. This also has its limits and risks, as the interviewee who raises the need to do database crossings.

This complexity has computerized safeguards, but a comprehensive legal support is needed which allows civil servants a greater guarantee and support on their actions, as well as establishing sanctions in case of non-compliance of procedures and protocols.

In relation to the principles of quality and safety, there is the issue of **infrastructure** which allows the maintenance and protection of databases. There are clearly two types of institutions, some with an IT department with 20 or more people, while others with a much lower number of around 10 people.

The paradigm shift from paper to digital data, from physical folders to relational databases, has been developing in different ways in different areas of the State. What appears in the interviews is that some institutions work with an inadequate number of IT experts and this can increase the risk factors in some cases.

Conclusions and recommendations

The findings from the interviews to civil servants and experts from the State institutions show a mixed picture regarding the existence of adequate standards and practices of protection of personal data contained in public databases. While there are evidences of the application of some good practices, the absence of a strong regulation which applies to all institutions is the main problem found and that exposes citizens whose data are stored at risk.

The people in charge of databases have a very low level of familiarity with protection standards, whether they are internal, national or international regulations. Some of them are ruled by the decrees of establishment of the institutions and others by “unwritten rules”. There is also a slight tension with the scope of Act 5282/14 of access to public information. In absence of an updated and comprehensive Act of personal data protection, each institution establishes or solves on its own the tensions that are generated by Act 5282/14 when providing information. It can be inferred that the exceptions established in the regulation of the Act on access to public information are unknown or not taken into account when settling disputes.

Another principle that is not met according to the findings from the interviews is to establish a limit to the storage of personal data. Almost all institutions lack protocols, mechanisms or regulations for the destruction of such data. They indicate several reasons for not doing so. However, criteria should be established depending on the nature of the database.

There are doubts about the application of the principles of notification, specification of purpose and limitation in use. Most of the interviewees affirm that they let people know when their data are being collected and for what purposes. What is not clear is whether institutions notify by principle of personal data protection or by satisfying an operational need to collect data of potential beneficiaries of social programs, for example.

On the specification of purpose, although some interviewees explain that data are collected to meet the objectives and activities of the institutions, the statements are vague when there are no specific rules or regulations which regulate the collection of personal data.

Regarding the limitation in the use of the data, even though civil servants say that their institutions use the data strictly for the purpose they are collected for, again the absence of specific regulations raise doubts about the spirit and effectiveness of the application of this principle.

It emerges from the interviews that institutions have mechanisms to update the data, which is directly linked to the quality of the data. Most of the civil servants were specific in explaining how these mechanisms work in case the data are erroneous or need changes over time. It can be inferred that the institutions interviewed comply with this principle.

As far as access and transfer of data, the application of good practices can also be identified. Most of the interviewees admit having strict data access policies with established roles and, in some cases, with registry of access.

In terms of transfers, several ways of data exchange among public sector bodies are identified without a regulatory framework where protocols and procedures are established to safeguard these exchanges. The mechanisms of exchange are varied, although there is a tendency of doing them in a systematic and centralized way to avoid duplication of information and proliferation of databases in different institutions.

On the creation of an Act for personal data protection

The right to protection of personal data derives from the right to privacy. A legislation on this topic should regulate the way in which public and private data of individuals are collected, processed, stored and removed electronically or analogically from public and private sources.

Personal data must be treated for the determined or specific purposes based on the consent and informational self-determination of each data subject and with some legitimate and legal basis that transcends such need. In addition, ARCO rights must be included for the compliance of the protection standards.

Paraguay has many regulations which cover the processing of personal data: collection, use and authority of application for each case. However, an Act with a comprehensive approach is necessary and urgent to avoid possible abuses that occur with personal data both in the public and private sector. This Act should limit the processing of personal data with respect to collection, storage time, proportionality, quality of data, scope of application, transparency, accountability and other principles established by the highest standards of personal data protection with a human rights perspective, used by the Directive 95/46 of the EU and its regulations. Also, the future Act of personal data protection should contemplate technological advances: biometric data, algorithms, big data, and international data transfers, among others.

It will be necessary to create an independent body as the governing body and responsible for the control of data processing, to analyze the purpose of them and to make preventive reviews of possible errors or abuses that occur in data processing. It is necessary to audit data controllers and raise the standards for data protection, in accordance with the EU Directive 95/46. In absence of a supervising body, the retention of traffic data can adversely affect the privacy of people and counteract the effort that customers or users must do to protect their information from possible abuses or errors that may be committed, as well as other current regulations exposed in the legal analysis of this research, that their form of collecting information and personal data is unknown.

Likewise, the Act should not create obstacles to the progress of Act 5282/14 of access to public information. It should contain legal provisions which ensure access to personal data when public interest is greater than the need for confidentiality, such as the disclosure of salaries of civil servants, for example.

One of the challenges in the common agenda of working groups in international forums is the debate on the personal data protection directly related to fundamental rights such as freedom of expression and privacy. Paraguay is part of these international networks and organizations seeking a balance between these rights including exceptions and provisions on considerations relating to public interest and new scenarios as the digital economy. The challenge is to force from the citizens the compliance of the commitments made in these areas: OECD, UN, MERCOSUR, Personal Data Protection Network, among others.

Bibliography

2013 OECD Privacy Guidelines - OECD. (n. d.). Recovered 15 February 2017, from https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

ABC Color. (n. d.). Special - TheCecilia Cubas Case - ABC Color. Recovered 15 June 2017, from http://www.abc.com.py/multimedia/caso-cecilia-cubas/

Constituent Assembly. (1992). National Constitution of the Republic of Paraguay. Recovered 20 January 2017, from http://www.bacn.gov.py/constitucion-nacional-de-la-republica-del-paraguay.php

Cerda Silva, A. (2011). Informational self-determination and Acts on data protection. *Chilean Magazine of Digital Law*, *0*(3). https://doi.org/10.5354/0717-9162.2003.10661

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

CIDH. (2009, July 6). Case of Escher et al. v. Brazil. Sentence of 6 July 2009. Recovered from http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

National Commission of Telecommunications (CONATEL). Resolution 1350_2002. By which the Obligation to register the call detail record for a period of six (6) months is established. Recovered from http://www.buscoley.com/pdfs/r_1350_2002.pdf

National Congress. CODE OF JUDICIAL ORGANIZATION (1981). Recovered from http://www.pj.gov.py/descargas/ID1-60_id482_codigo_organizacion_judicial.pdf

National Congress. ACT N°125/91 WHICH ESTABLISHES THE NEW TAXATION REGIME (1991). Recovered from http://www.oas.org/juridico/spanish/mesicic3_pry_ley125.pdf

National Congress. Act Nº 1682/01 Which Regulates private information, 1682/01 § (2001). Recovered from http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=1760

National Congress. Act Nº 1969/2002 WHICH MODIFIES, EXTENDS AND REPEALS ACT N° 1682/2001 «WHICH REGULATES PRIVATE INFORMATION», 1969/2002 § (2002). Recovered from http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=2539

National Congress. Act Nº 5282 of Free Citizen Access to Public Information and Governmental Transparency (2014). Recovered from http://informacionpublica.paraguay.gov.py/public/ley_5282.pdf

Fuenzalida Bascuñán, S. (2015). The jurisprudence of the Inter-American Court of Human Rights as a

source of law: A revision of the doctrine of “exam of conventionality”. *Law magazine (Valdivia)*, *28*(1), 171-192. https://doi.org/10.4067/S0718-09502015000100008

Jorge Rolón Luna, Maricarmen Sequera Buzarquis. (2016, March). State Surveillance of communications and fundamental rights in Paraguay. Recovered from https://www.tedic.org/wp-content/uploads/sites/4/2016/05/Paraguay-ES.pdf

Act N° 642/95 “On telecommunications”. (n. d.). Recovered 22 March 2017, from https://www.conatel.gov.py/images/iprincipal/LEY%20642/Ley_N_642-95.pdf

MERCOSUR. (2008). XX ORDINARY MEETING OF THE WORKING SUB-GROUP N° 13 “E-COMMERCE”. Recovered from http://www.mercosur.int/msweb/SM/Noticias/Actas%20Estructura/DEPENDIENTES%20DEL%20GMC/Subgrupos%20de%20Trabajo/SGT%2013/2008_ACTA01/Acta0108.doc

Montoya Melgar, A. (1995). *Basic legal encyclopedia*. Madrid: Cívitas.

OAS. Vienna Convention (1961). Recovered from http://www.oas.org/legal/spanish/documentos/convencionviena.htm

OAS. American Convention on Human Rights Subscribed in the Specialized Inter-American Conference on Human Rights (B-32), B-32 § (1969).

UN. (1948, December 10). Universal Declaration of Human Rights. Recovered from http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

UN. (1966, December 16). International Covenant on Civil and Political Rights. Recovered 20 January 2017, from http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

UN. A/RES/45/95. Guidelines for the regulation of computerized personal data files (1995). Recovered from http://www.un.org/documents/ga/res/45/a45r095.htm

ONU. Privacy in the Digital Age (2016). Recovered from http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

Pappalardo Zaldívar, C. (1992). *Constitutional reform*: *projects and contribution*. Asunción: Vive : Intercontinental.

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

Rodríguez Palop, M. E., & University Carlos III of Madrid. (2002). *The new generation of human rights: origin and justification*. Madrid: University Carlos III of Madrid, University Institution of Human Rights «Bartolomé de las Casas» : Dykinson.

European Union. Directive 95/46/CE of the European Parliament and the Council, of 24 October 1995, relating to the protection of natural persons regarding personal data processing and free flow of these data 95/46/CE § (1995). Recovered from http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A31995L0046

Annexes

A.1. Interview Script

The following definition of Database was read at the beginning of each interview, due to the ambiguity of the current legislation and it was helpful to have a common conceptual framework with the interviewee:

> *"[...] an organized set of data which are managed or processed, electronic or not, regardless of the type of formation, storage, organization or access, whose owner is a legal person of public nature".*

These are the guiding questions that were used in the interviews.

Nature of databases

- What public databases do you manage?? Which one/s are under your responsibility?
- What type of data are in those databases?
- What personal data are in those databases?

Application of protection principles

- What legal, regulatory instrument authorizes the collection of that data? (principle of collection)
- Are people notified for the collection of their data? (principle of collection)
- Why are these data stored? (principle of collection; principle of specification of purpose)
- Are these data used for other purposes other than the original ones (archive purposes, scientific studies, etc.? Are they imparted, shared or published beyond the original collection purposes? (principle of limitation in use)
- Are these data updated? How? (principle of quality)
- Are these data modified in case they are erroneous? How? (Rectified, deleted)? (principle of quality, principle of individual participation; accuracy)
- Are these data deleted at any time? After a certain time? For what reasons? In case they are not deleted, why? (limitation of conservation period)

Regulations, protocols of use and processing of databases (principle of security)

- What regulations are applied for the personal data protection? Internal regulations of the institution? National regulations taken into account?
- What risks of the database security are identified? (legal, technological, human)
- Do you remember any incidents where data security was compromised? How did you manage the situation?
- What is the protocol you have in case the security of the databases is compromised?
- What is the standard used for information security? Do you use the ISO 27001 standard?
- If the answer is no, what is the information security procedure?

Authorization of access and transfer to the bases

- Who is authorized to access these databases? Is there a monitoring or registry of accesses to databases?
- Why are these databases accessed?
- Are databases transferred? Why are these data transferred? How are they transferred (from the IT point of view)?
- Are the transfers national and/or international?
- Is there a protocol for the delivery of information to criminal prosecution authorities? Is it requested by note of the institution or by court order?

Infrastructure

- How many people work in the unit that maintains the infrastructure that supports the databases?

"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