



DATA PROTECTION IN LATIN AMERICA

Opportunities and Challenges for Human Rights

VOLUME I

Digital Area
Asociación por los Derechos Civiles



August 2017
<https://adcdigital.org.ar>

This report is published as part of a project funded by the Ford Foundation, and is licensed under Creative Commons Attribution-NonCommercial-ShareAlike.

To see a copy of this license, visit:

<https://creativecommons.org/licenses/byncsa/2.5/>



The report *Data Protection in Latin America. Opportunities and Challenges for Human Rights* is for public dissemination and has no commercial purpose.

Table of contents

I	Executive Summary	5
II	Context: The role of personal data	6
i	General notions	6
ii	Technological development	6
iii	Changes in organizational practices	8
III	Guidelines and international principles	9
IV	Distinction between privacy and personal data. The European General Data Protection Regulation	10
V	National norms: The situation in Latin America	12
i	General characteristics	12
ii	Comparative analysis of four countries in the region: Argentina, Chile, Brazil, and Mexico. Their correspondence with international standards	14
i	Preliminary considerations	14
ii	Methodology	15
ii.1	Regulatory Framework	16
ii.2	Definitions	17
ii.3	Principles on data processing	19
ii.4	Consent	21
ii.5	Data subject's rights	23
ii.6	Responsibilities and obligations of those who process the data and the related subjects	25
ii.7	International data transfer	26
ii.8	Application and enforcement mechanisms	28
ii.8.1	Enforcement and controller authority	28
ii.8.2	Sanctions	29
ii.8.3	Actions and resources	30
ii.8.4	Compensation (damages)	30

Data Protection in Latin America: Opportunities and Challenges for Human Rights*

I Executive Summary

In this document, Asociación por los Derechos Civiles analyzes the regulatory systems for data protection in Argentina, Brazil, Chile, and Mexico both in comparison to each other and in comparison to the General Data Protection Regulation (GDPR) in the European Union. The purpose of this document is to identify opportunities and challenges for human rights in light of the role which personal data has taken on by virtue of contemporary technological development.

This project was completed thanks to research carried out by Asociación por los Derechos Civiles (ADC) in Argentina, InternetLab in Brazil, Derechos Digitales in Chile and Red en la Defensa de los Derechos Digitales (R3D) in Mexico, mentioned in point 5.5.2.

The document begins with an explanation about the emergence of legislation regarding data protection and its ongoing expansion, a product of technological development and the emergence of business practices which have placed the processing of personal data at the center of the business model of many companies. Then, it addresses the birth of international standards which seek to regulate and neutralize the potential injuries that the processing of personal data can cause to the rights of people.

It mentions the development that data protection had in Europe since its appearance as an autonomous right — distinct from other rights like privacy — through the adoption of the new General Data Protection Regulation (GDPR) by the European Union. After this review, it turns to the core

*This report was written by **Valeria Milanés**, Privacy and Freedom of Expression Areas Director, Asociación por los Derechos Civiles (ADC). Design and layout by: **Leandro Ucciferri**, lawyer and researcher, Privacy and Freedom of Expression Areas, ADC. This is a translation of the original report "*El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos*", published in December 2016 in Spanish, available at: <https://adcdigital.org.ar/portfolio/sistema-proteccion-datos-personales-latam/>. The report was translated by **Emmet Dymond Hollingshead**, volunteer at ADC during April and July 2017. Emmet is a Political Science and International Studies major at Macalester College in St. Paul, Minnesota.

of the project: a comparison between the regulatory dispositions of the four above-mentioned Latin American countries, with the goal of detecting similarities and differences in data protection regimes. In addition to the comparison between countries, these regulatory regimes are also compared to the GDPR due to the high protection standards which it establishes and its approach to the phenomenon of new technologies.

Finally, this document offers conclusions and recommendations, the objective of which are to establish a starting point for all concerned parties in the debate regarding the best ways to improve the defense of personal rights in the face of possible abuses in personal data processing.

II Context: The role of personal data

i General notions

The first norms linked to the protection of personal data privacy originated in the 1960s and 1970s, at the early stages of technological development.

Following analysis which the Organization for Economic Co-operation and Development (OECD) completed upon the update of the Guidelines for the Protection of Privacy and Transborder Flows of Personal Data in 2013¹, more than 30 years later, the advances in the technological and digital environment have been overwhelming. The volume of data and the uses of that data have exploded due to increasing simplicity in the collection, storage, processing, aggregation, analysis and transfer of huge amounts of data.

Advances in computing power combined with easy access to fixed and mobile devices which are globally connected through the Internet have transformed the role of personal data in the economy and society. The change from analog to digital technologies in communications and entertainment has resulted in a greater capacity to collect and share personal data, particularly photographs, audio files, films, and videos.

Personal data is increasingly the central asset for business operations and effective government administration.

ii Technological development

Diverse technological developments deepen this marked tendency of collection and use of personal data.

¹ "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" by the Organization For Economic Cooperation and Development - OECD (2013), p. 81 et seq. Accessible at <https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>

Communication networks based on computers connected on the Internet, as well as the various possibilities of connection via satellite, cable and fiber optic have increased capacity to access and transfer data. New devices, a greater interoperability and enormous growth in wireless technologies have also contributed to the increase in the data transfer rate.

The increase in the number of personal computers in homes and workplaces has reached dizzying speeds, and more recently, mobile devices have emerged, including smartphones. These particular devices, powerful and portable, combine data geography and Internet connection, which allows the development of a wide range of new services and applications, many of which rely on the collection and use of personal information to generate profits. In addition to Internet access, many of these devices contain tools that allow the capture of images, sound, and location data. The potential of these devices to capture and distribute images and to track the location and the movements of individuals, often without their knowledge, have grown significantly.

Furthermore, the costs of digitized storage have dropped significantly, so that data can be saved for long periods of time, or even indefinitely. The volume of personal data maintained by organizations and individuals has also expanded. Storage practices are evolving as organizations and individuals use storage services provided by third parties, whose databases may be located in other countries.

Data processing tools are increasingly powerful, sophisticated, ubiquitous, and cheap, which makes the information easy to find, link and locate for various actors, not just governments or large corporations.

The development and use of algorithms and analytical tools have allowed access to enormous data sets and have made it possible to connect these data, which results in new uses, thus making the information even more valuable. Automated decision-making through data mining and algorithms is possible in ever more contexts.

The phenomenon of *big data* — a term used to refer to huge amounts of data that can be stored, linked and analyzed — brings with it the possibility of finding information, trends and knowledge which otherwise would not have been obvious or could not have been reached.

To this we can add wireless networks, which allow interaction between the individuals or computers and the environment that surrounds them. These networks have seen more rapid and more extensive development in areas such as medical care, the environment, the transport system, and the development of energy control systems.

Radio Frequency Identification (RFID) enables wireless collection of data through devices which identify attached or embedded electronic tags on objects, whether for identification or for other purposes. The use of RFID systems requires software, networks and databases which allow information to be transferred from the tags to the organization's information infrastructure using RFID, where it is processed and stored. RFID can be used for transport, identification cards, passports

or commercial sale — its uses are quite varied. Electronic tags may contain personal data, and, depending on the strength of the reader and the types of protections applied to the data, they can be read. This, depending on the specific RFID and its configuration, may expose personal information to third parties.

Mobile devices, whether through a Global Positioning System (GPS) or the use of more sophisticated software, can provide information about whereabouts of an individual and their movements, thus allowing the development of personalized services and measure, and also targeted advertising. The combination of diverse sources of information, such as mobile devices, RFIDs enabled on transport cards, surveillance cameras and other source data, if combined, can link an individual and their habits.

The technological development that allows the human body to become a source of information has also been notable. Advances in medical technology to prevent and treat diseases, estimate health risks, or establish biological links have been significant. Organizations have also started to collect biometric data for use in a growing variety of contexts, mainly as a means of identification and authentication.

iii Changes in organizational practices

To understand the current context, it is also important to mention some of the changes identified by the OECD in the aforementioned document, and changes that have occurred in the practices of the private sector, the public sector, and individuals themselves as a result of these new technological circumstances.

The private sector has changed its business model. International data transfers in sectors such as human resources, financial services, education, electronic commerce, are an integral part of the global economy. Data transfers are virtually instantaneous and without cost. Simply by pressing a key or clicking a mouse button one can move data quickly and easily around the world. The result is that organizations have greater flexibility, mobility, and storage capacity, while reducing costs at the same time. This type of technology is not only accessible to large multinational organizations, but also to small and medium-sized enterprises, as well as individuals, who can use global storage services, processing, and transfer of data, often involving multiple different providers.

New business models based exclusively on personal data have also been generated. Technology has enabled individuals to share personal information very easily. There exist organizations which provide platforms for user-generated content, usually without direct cost, and then seek to generate income from that user's personal information. Profiling, behavioral targeting, and the segmentation of audiences occur on an ever-larger scale.

The public sector has also used technological changes and more efficient personal data processing to carry out or improve certain government services and operations. The ability to access personal data in such a way has changed the way the public sector uses the Internet to inform and engage the public. Diverse government agencies and enforcement authorities often use social networks as they seek public participation in the creation of public policy.

The public sector has begun to request or require the private sector to withhold and deliver certain personal information, through a legal orders and for public policy purposes.

Finally, it is worth noting the changes in practices developed by individuals themselves. More and more people conduct business transactions online, including purchases, transactions banking and travel. In each of these transactions, the individual shares a great deal of information with the organizations with which they interact.

Likewise, the development of various applications has allowed individuals to generate and share information, usually personal information, but often from family and friends as well. The new tools and services available to Internet users have generated a change in their online behavior. Personal data is usually given voluntarily by individuals, without being directly requested by the organizations. Many individuals have their own blogs, share photos and videos online, perform commercial operations, and interact with large numbers of friends or public groups on social networking sites.

III Guidelines and international principles

The complexity and abrupt change generated by technological development and personal data's corresponding strategic role have also generated a series of concerns about the violation of individuals' essential rights. Mainly regarding the right to privacy and informational self-determination, these concerns also touch upon rights such as non-discrimination, freedom of expression, thought, and opinion, and freedom of assembly.

As such, various agencies and international bodies have generated diverse ways to address this concern. These groups are of global and regional capacity, hail from governmental and civil origins, and bring expertise in law as well as the relevant technology.

The instruments which these groups have developed are of many different types and scopes. In most cases they are presented as guidelines or suggested principles, and in other cases they are presented as legislation for immediate use by lawmakers. It should also be noted that these instruments seek to harmonize the impact of one or several of the rights mentioned above with other interests, and are linked to their own sphere of action.

As a non-exhaustive list, examples of principles and guidelines elaborated as proposals or suggestions to be implemented by different actors, depending on the type of organization concerned, include:

- Guidelines for the Regulation of Computerized Personal Data Files by Resolution by the General Assembly of the United Nations.²
- Resolution on The Right to Privacy in the Digital Age adopted by the General Assembly of the Organization of the United Nations in 2016, which modified and updated previous positions.³
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organization for Economic Co-operation and Development (OECD), which were initially published in 1980 and updated in 2013.⁴
- Proposed Declaration of Privacy Principles and Protection of Personal Data in the Americas adopted by the Inter-American Juridical Committee of the Organization of American States (OAS).⁵
- Privacy Framework by Asia-Pacific Economic Cooperation (APEC).⁶
- Privacy Considerations for Internet Protocols, Request for Comments N° 6973 of the Internet Engineering Task Force (IETF), written by the Internet Architecture Board (IAB).⁷
- International Standards on Data Protection and Privacy adopted in The 31st International Conference of Data Protection and Privacy Authorities.⁸
- Privacy Standards in a Global World, Civil Society Statement of 3 November 2009 in Madrid, Spain.⁹

IV Distinction between privacy and personal data. The European General Data Protection Regulation

There will be no mention in this document of the various international treaties which contain provisions concerning the privacy or protection of personal data, since the study of such treaties in research related to this subject is profuse.¹⁰

² Accessible at <http://www.un.org/documents/ga/res/45/a45r095.htm>

³ Accessible at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

⁴ Accessible at <http://bit.ly/1Ot27bJ>

⁵ Accessible at http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

⁶ Accessible at <http://bit.ly/1zRV0QK>

⁷ Accessible at <https://tools.ietf.org/html/rfc6973>

⁸ Accessible at <http://bit.ly/2kMYwZA>

⁹ Accessible at <http://thepublicvoice.org/madrid-declaration/es/>

¹⁰ An example is the American Convention on Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights or Convention 108 of the Europe for the protection of persons with regard to the automatic processing of personal data.

However, it is worth clarifying that in Europe, the right to the protection of personal data is recognized as legally distinct from the right to privacy. Several national constitutions contain distinctive provisions in this respect and, moreover, the Charter of Fundamental Rights of the European Union, adopted on December 7, 2000, establishes a clear distinction between one right and the other. While Article 7 enshrines the right to life private and family life, Article 8 recognizes that everyone has the right to the protection of personal data.

Later, and without intending to carry out an analysis of the normative dynamics of the European Union and/or the Council of Europe with each other and with their Member States, the General Data Protection Regulation, issued by the European Parliament and the Council of Europe on April 27, 2016 will be taken as an example of a direct application of these rights. This Regulation (EU) N° 2016/679 protects individuals in personal data processing and the free circulation of data.¹¹

The Regulation, which has already been passed by the legal authorities, will be applicable from May 25, 2018 onwards in all of the countries which make up the European Union (EU). It surpasses — in application and in guarantees related to informational self-determination and protection of personal data — Directive 95/46/EC, which it repeals. In several ways, the adoption of Regulation also responded to the changes described in section 2.1.

The EU recognizes that personal data processing must be conceived to serve humanity, and it therefore holds the protection of natural persons in personal data processing as a fundamental right. It also considers that the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and maintain a balance with other fundamental rights, in accordance with the principle of proportionality. The Regulation, as set out in its recitals, respects all fundamental rights and observes the freedoms and principles recognized in the Charter of Fundamental Rights of the European Union, in particular private and family life, of the home and communications, the protection of personal data, freedom of thought, freedom of consciousness and religion, freedom of expression and information, freedom of business, the right to effective judicial protection and a fair trial, and cultural, religious and linguistic diversity.¹²

The substantial increase in cross-border flows of personal data produced by greater economic and social integration, — which are themselves a result of the internal functioning of the market — as well as the increase within the EU in the exchange of data between public and private operators including individuals, associations and companies, highlights the relevance of developing market confidence to the development of the digital economy in the internal market. In addition, we should ensure a uniform and high level of protection for natural persons, and eliminate obstacles to the movement of personal data within the EU. To that end, the level of protection of rights and freedoms of natural

¹¹ Accessible at <http://bit.ly/2jRVq5P>

¹² Section (4) of Regulation (EU) 2016/679.

persons in connection with the processing of such data must be coherent and standardized.¹³

The previous Directive 95/46/EC, which lasted 20 years, allowed the EU to go a long way in protecting personal data, with bodies and entities exclusively dedicated to analysis, study, and resolution of related issues, such as the Article 29 Working Party¹⁴ or the European Data Protection Supervisory Authority.¹⁵

Regulation 2016/679 (EU) will have scope beyond the borders of the EU. On the one hand, it affects companies that, although they have no establishment in the EU, offer their products there. On the other hand, the Regulation provides for the periodic review of adequacy¹⁶ granted by the European Commission to outside countries receiving data transfers from the EU.

Pending its full implementation, the Regulation proves to be a valuable example in terms of its purpose as a supranational normative harmonization of the direct application, strong guarantee, and protection of human rights with special emphasis on informational self-determination, which guarantees that natural persons to have control of their own personal data.

V National norms: The situation in Latin America

i General characteristics

Following Cerda Silva,¹⁷ Latin American legal systems, while sharing the tradition of European continental civil law, have also recognized the right to privacy and the right to the protection of personal data as separate legal entities.

The right to data protection has constitutional recognition. In general, the constitutions of the region recognize the right to privacy, but the constitutions of Argentina, Brazil, Colombia, Mexico, Peru and Venezuela also include the so-called resource of *habeas data*, which is the right to the protection of personal data. But even if this provision is not expressly contained in the constitutional texts, the relevant courts have recognized the right to control one's own information.

Thus, this document emphasizes that Latin American constitutionalism has been comparatively more efficient in protecting the right to the protection of personal data, and identifies three areas of focus:

¹³Sections (5), (7) and (10) of Regulation (EU) 2016/679.

¹⁴<http://bit.ly/2gs7BE2>

¹⁵<https://edps.europa.eu/>

¹⁶The adequacy of the European Commission mandates that the receiving country has adequate protection of the personal information; such is the case of Argentina and Uruguay, among others.

¹⁷Towards a Free Internet of Censorship: Proposals for Latin America. Chapter 4. Protection of personal data and provision of online services in Latin America. Author: Alberto Cerda Silva. Compiler: Eduardo Bertoni. Center for Studies in Freedom of Expression and Access to Information of the Faculty of Law of the University of Palermo. Accessible at http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf

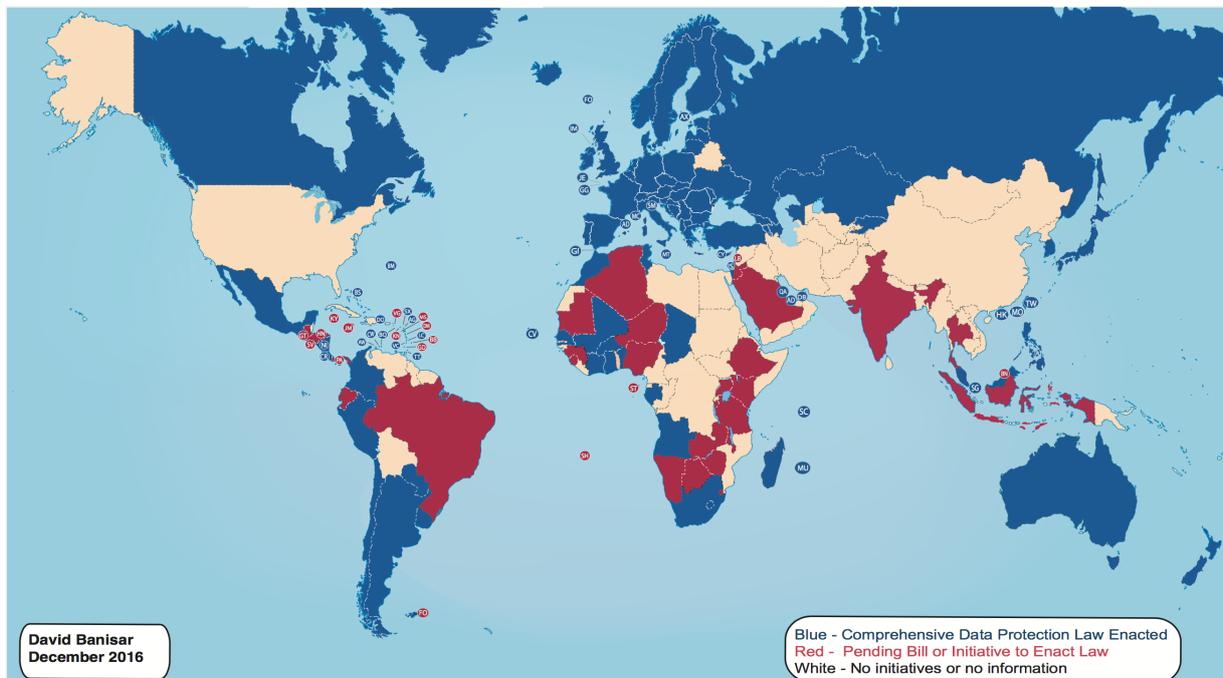
- Recognition of the right to the protection of personal data as an autonomous right;
- The provision of constitutional avenues to procure such protection;
- And, following the European constitutional tradition, by recognizing such a right and providing for its protection not only in relation to the public sector, but also against non-state actors.

However, constitutional protection is not sufficient, due to causes quite common in the región such as high transaction costs, inefficiency in preventing non-compliance, and lack of *stare decisis* in judicial decisions — since, except for certain exceptions which will be named, their application in a case is subject to judicial decision. Add to this that constitutional provisions are very general, leaving much room for judicial interpretation. As such, when applied to specific cases they can generate ambiguous or incorrect decisions with a lack of legal certainty.

Latin America in general adopted comprehensive laws for the processing of personal data during the 1990s. These laws regulate the automatic and manual processing of personal data by both the public and private sectors. Latin America has also followed the European tradition of comprehensive protection, unlike the United States, whose protection is fragmented by sector and is very succinctly based on privacy criteria and high sensitivity data, not informational self-determination.

The following map by David Banisar¹⁸ shows (in blue) countries that have comprehensive data protection laws in Latin America and the rest of the world.

National Comprehensive Data Protection/Privacy Laws and Bills 2016



¹⁸Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2016 (November 28, 2016). Available at SSRN: <https://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416>

In his work, Cerda Silva pointed out that the Latin American data protection regime is in a transitional phase. Most major economies in the region have constitutional protections and comprehensive protection laws that regulate the processing of personal data in both the public and private sectors. Thus, in general terms, data protection in Latin America appears robust. However, countries still need to work to make these laws effective and respond to the current challenges which arise from technological development and the growing international transfer of personal data.

ii Comparative analysis of four countries in the region: Argentina, Chile, Brazil, and Mexico. Their correspondence with international standards

i Preliminary considerations

The previous section will be illustrated by comparative analysis of the data protection systems of four countries in the region: Argentina, Chile, Brazil and Mexico. The last three countries were selected because they are in the process of reforming their regulations.

The analysis will include the correspondence of the characteristics of each of these systems with the standards advocated by the European system of protection of personal data.

The selection of the European system as an international reference was due to several reasons, among them:

- Latin American legislations have been developed largely following the inspiration of the European system;
- The countries of the region have adopted, in line with the European system, the distinction between the right to privacy and the right to informational self-determination, as different legal entities;
- The European system for the protection of personal data has a harmonizing vocation and contains references to the protection of other human rights and the free flow of data aimed at enabling the development of the digital economy;
- Several of the countries of the region have adopted protection systems inspired by European regulations, in particular by Spanish legislation;
- Since 2003, the Ibero-American Network for the Protection of Personal Data, which coordinates between organizations which work for data protection, other organizations with a similar focus, and with Latin American countries, among many other activities, has held 15 annual meetings. In addition to Spain, between members and observers, 14 Latin American

countries have participated in this network, as well as the European Monitoring Protection of Personal Data on behalf of the European Union and other international bodies as observatory participants;

- At least two countries in the region (Argentina and Uruguay) have been declared suitable countries by the European Commission, therefore their systems of protection of personal data already aligned with the European standards initially envisaged by the previous Directive 95/46/EC;
- For the most part, Uruguay has formalized its adherence to Convention 108 of the Europe for the Protection of Individuals with regard to automated data processing of a personal nature in August 2013.

For a full understanding of the situation in each of the countries selected, we rely upon the invaluable contribution of colleagues from civil society organizations, who during the years 2015 and 2016 carried out an analysis of their internal regulations and their correspondence with European standards.

The organizations which produced those reports were *Derechos Digitales* in Chile, *InternetLab* in Brazil, *Red en Defensa de los Derechos Digitales* in Mexico, and that of Argentina was made by Eduardo Ferreyra of Asociación por los Derechos Civiles.

Finally, the Proposal for the Declaration of Principles of Privacy and Data Protection in the Americas, adopted in 2012 by the Inter-American Juridical Committee of the Organization of American States (OAS), deserves a separate comment.¹⁹ While the principles are intended to guide the development of the legal systems for the protection of personal data in the countries which make up the OAS, which obviously includes the countries of Latin America, they are not the international standards which we use here. This is because the principles adopted by the Legal Committee establish a very low level of protection, falling below the systems in force in several countries of the region and very far from the standards of data protection promoted by the European system, whose characteristics have already been delineated.

ii Methodology

Due to their abundance of information and understanding, we used the country reports from each of these organizations, as listed below. The reports were prepared between 2015 and 2016.

- The Argentina report is available at the following link: <https://adcdigital.org.ar/wp-content/uploads/2017/argentina-sobre-proteccion-de-datos-personales-ADC.pdf> (in Spanish)

¹⁹ Available at http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

- The Chile report is available at the following link: <https://adcdigital.org.ar/wp-content/uploads/2017/01/de-datos-personales-en-Chile-Derechos-Digitales.pdf> (in Spanish)
- The Mexico report is available at the following link: <https://adcdigital.org.ar/wp-content/uploads/2017/01/de-datos-personales-en-Mexico-R3D.pdf> (in Spanish)
- The Brazil report is available at the following link: <https://adcdigital.org.ar/wp-content/uploads/2017/01/Protection-in-Brazil-InternetLab.pdf>

After a brief analysis of the main characteristics of the regulatory frameworks of each country, each of the following elements will be addressed: definitions; principles relating to data processing, consent; rights of the data controller or data subject; responsibility and obligations of the data user and other related parties; transfer and assignment; mechanisms for application and enforcement such as application and control authority, sanctions, possible actions on the part of the data subject, and compensation for damages.

With respect to the items outlined, the main characteristics of each one will be highlighted according to the European system²⁰, and the outstanding features of the countries under analysis will be highlighted. Where relevant, each item will be illustrated with a comparative table of the four countries.

We emphasize that the aspects selected tend to cover general assumptions, so that in the following analysis there will be no mention of the particular processing of certain data, such as sensitive data, financial data, advertising data, data held by the police and security forces, etc.

ii.1 Regulatory Framework The four countries under analysis enshrine the right to privacy in their constitutions, and three of them contain provisions regarding the right to the protection of personal data — Argentina and Brazil insofar as they refer to habeas data and Mexico as a right in itself. For its part, Chile, although it does not expressly mention it, has generated an alternative recognition of personal data as a separate figure from the right to privacy through case law.

Argentina, Chile and Mexico have comprehensive data protection laws. Argentine law dates from the year 2000 and Chilean law was enacted in 1996. To a greater extent, Mexico has a specific law for the private sector of 2010 and a recently approved law (December 2016) specific to the public sector.

Brazil does not have a specific law for the matter or a system for the protection of personal data. However, some provisions regarding different types of personal data can be found in different laws and regulations. As such, references to the protection of telecommunications data are identified in the General Telecommunications Law, Anatel resolutions (a telecommunications regulator), the

²⁰The European General Data Protection Regulation N° 2016/279. Accessible at <http://bit.ly/2kdyleT>

Internet Civil Registry and its regulatory decree, interceptions law, criminal organizations law and the criminal code. There are also references to consumer data, financial data and health data in specific regulations in each of these sectors.

It should be added that Argentina is in a process of reflection for the reform of the current law²¹, and that Chile is awaiting the presentation of a bill by the government which is integral, comprehensive, and overcomes the current deficit deficit. Chile has already seen several other bills introduced to Parliament, which mostly address particular and specific aspects, such that they suffer from a lack of comprehensive vision regarding the data protection system.

Brazil has also reported on the need for a comprehensive data protection law, and through a process of collective participation initiated by the Ministry of Justice, a bill was drafted, No. 5276 of 2016, which was presented to Congress in May of that year. Given the importance of this project, the bill will be included in the following analysis.

Regulatory framework	Argentina	Chile	México	Brasil
Constitution				
Privacy	+	+	+	+
Personal data/habeas data	+	-	+	+
Data Protection Law	+	+	+(2)	-

Table 5.1.- Comparison of the regulatory framework²²

ii.2 Definitions The European General Data Protection Regulation (GDPR) contains a wide catalog of definitions about concepts that are considered decisive for regulating personal data processing and which reflect the current complexity of the numerous variables in the personal data processing, such as the multiplicity of subjects, the various types of data, and the technological environment.

In this sense, the true list is much longer than the ones provided by the laws in Argentina and Chile, which are based on a modest list of concepts which mostly covers definitions linked to subjects and data processing. However, in general, the definitions contained in the laws have similar characteristics. The exception is Mexico, whose regulations contain a long list of definitions, including terms like “cloud computing” and others with a rather technological tenor.

By way of illustration, among the concepts incorporated in the Regulation but not included in the laws in force in the countries under study (except Mexico, which in some cases considers them) are:

²¹ [http://www.jus.gob.ar/datos-personales/comunicados/2016/12/19/aportes-sobre-la-necesidad-de-una-reforma-a-la-ley-sobre-proteccion-de-los-datos-personales-\(1\).aspx](http://www.jus.gob.ar/datos-personales/comunicados/2016/12/19/aportes-sobre-la-necesidad-de-una-reforma-a-la-ley-sobre-proteccion-de-los-datos-personales-(1).aspx)

²² Comparative table of own elaboration.

limitation of processing, profiling, genetic data, biometric data, company, corporate group, binding corporate rules, and service of the information society.

Next, four definitions will be briefly analyzed in particular: personal data, sensitive data, processing, and owner.

In relation to the concept of personal data, Argentina, Chile and Mexico share similar definitions, as they relate to the data of identified or identifiable natural persons (Argentina also includes people of ideal existence).

This notion is related to the proposal in the GDPR. However, the definition of personal data in the Regulation goes further and establishes that a person will be considered identifiable when his identity “can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”²³

Brazil’s sectorized legislation lacks a definition of personal data despite being mentioned in different regulations (such as the Civil Internet Framework). Bill 5276/2016 attempts to remedy this omission, in a manner similar to that provided by the GDPR.

The four countries under review contain similar definitions of sensitive data, which are in line with the GDPR provisions. The Regulation, which refers to sensitive data as “special categories of data processing”, includes a number of different types of data already provided for by the laws of the countries concerned, namely data showing ethnic or racial origin, political opinions, religious or philosophical convictions, trade union membership, and data relating to the health or sexual life of individuals. However, it also incorporates some types of data such as genetic data (also included in Mexican legislation) and biometric data aimed at uniquely identifying an individual.

It should be noted that in the case of Brazil, the definition of sensitive data is found in the Financial Records Act. For its part, bill 5276/2016 incorporates a definition aligned to the Regulation.

It is important to note that there is also quite an overlap in terms of the activities included under the concept of “processing”, as this term refers to any operation or set of operations, whether automated or not, such as harvesting, conservation, ordering, storage, modification, relationship, evaluation, blocking, destruction, transmission, assignment, etc. The Argentine, Chilean, and Mexican laws contain a definition of processing; Brazil’s law does not, although the project 5276/2016 does contain such a definition.

Regarding the person which the data is about - called “data subject” in the GDPR - there is also an overlap where there is any physical person or natural person whose data is involved. This criterion can also be inferred in Brazil, by virtue of the definition of sensitive data contained in the financial

²³http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf page 33.

records law, and is also included in bill 5276/2016. The exception is Argentina, which also includes legal or natural persons.

Definitions	Argentina	Chile	México	Brasil
Personal data	+	+	+	-
Sensitive data	+	+	+	+/- (*)
Data processing	+	+	+	-
Data subject	+	+	+	-

Table 5.2.- Comparison of definitions. (*)Here we used +/- since the definition of sensitive data arises from a law that governs a specific sector, and not with general scope.²⁴

ii.3 Principles on data processing The GDPR contains a series of principles which should be observed in all personal data processing.

- Legality, loyalty and transparency: the data must be processed in a legal, fair and transparent manner in relation to the data subject. It should be understood by “legal” that the processing should be adjusted in accordance with the law. It should be further understood by “transparent” that the owner should be informed — upon the collection of the data — who is linked to the data and the corresponding address, what will be done with the data, its possible destinations, optional or obligatory character and the consequences of providing the data or not, the possibility of exercising certain rights, etc.;
- Limitation of purpose: data must be collected for specified, explicit and legitimate purposes and will not be further processed in a way incompatible with those purposes. Further processing of personal data for archival purposes in the public interest, scientific and historical research purposes, or statistical purposes shall not be considered incompatible with the initial purposes;
- Accuracy: data must be accurate and, if necessary, updated; All reasonable steps shall be taken to remove or rectify without delay personal data which are inaccurate in relation to the purposes for which they are being processed;
- Limitation of the storage period: data must be maintained in such a way as to allow identification of the data subject for no longer than is necessary for the purposes of the processing of personal data; personal data may be retained for longer periods provided that they are processed exclusively for the purpose of archiving in the public interest, scientific or historical research or statistical purposes;

²⁴ Comparative table of own elaboration.

- Integrity and confidentiality: data shall be processed in a manner that ensures adequate security of personal data — including protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage — through appropriate technical or organizational measures;
- Data minimization: data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In the Argentine law there exists a relative similarity between the principles enshrined in both legislations. Thus, the two legal systems recognize the principles of lawfulness, transparency, purpose, accuracy, necessity, confidentiality and limitation of the conservation period. However, the differences arise when determining the content of each of them. For example, for Argentine law the principle of legality is fulfilled when the database is registered in the Registry created for this purpose, in addition to observing the principles established in the law. For its part, the GDPR establishes a detailed and precise set of conditions of which at least one must be fulfilled to be considered legal treatment. Registration of the databases is not one of these requirements.

The Chilean legislation does not make an explicit listing of the principles applicable to data processing operations. However, at least three of the provisions of the law can be deduced: the principle of purpose, the principle of data quality and the principle of lawfulness.

Mexican law enshrines the principles of lawfulness and loyalty, consent, purpose, proportionality, quality, responsibility and information. The “privacy notice” is one of the most important elements of the scheme provided for in the regulations. It consists of a physical or electronic document, generated by the data controller and made available to the data subject, prior to the processing of their personal data (for the private sector) or from the moment which they collect their personal data (for the public sector) in order to inform the subject of the purposes for which their data will be used.

In Brazil, the Internet Civil Framework establishes two principles for data processing: the principle of transparency and the principle of purpose. The Regulatory Decree of the Civil Framework includes a reference to the principle of minimization and limitation in the term of conservation. The aforementioned bill 5276/2016 offers a series of principles aligned with European regulations.

The principles of minimization and proactive responsibility do not appear as such in the normative texts under study, except as mentioned in the previous section.

Principles	Argentina	Chile	México	Brasil
Lawfulness, loyalty and transparency	+	+	+	+/-(*)
Limitation of purpose	+	+	+	+/-(*)
Accuracy	+	+	+	-
Limitation on storage period	+	-	+	+/-(*)
Integrity and confidentiality	+	-	+	-

Table 5.3.- Comparison of principles (*)Here we used +/- given that the definition of the principles in question were detected in the Marco Civil de Internet, which is not a data protection law.²⁵

A few words should be devoted to the requirement to register databases, which in Argentina, for example, is a legal requirement for data processing. All databases, whether public or private, must be registered. Chile establishes the registration of its public databases. Mexican legislation creates a National Data Protection Registry²⁶ for public agencies. However, this measure does not refer to the registration of public databases but to the registry of best practice schemes implemented by agencies. Its goal is to make the process transparent and make the general public aware of the procedures for guaranteeing the right to the protection of data, regardless of the level of government.

Registry	Argentina	Chile	México	Brasil
Public databases	+	+	-	-
Private databases	+	-	-	-

Table 5.4.- Comparison of Database Registry²⁷

ii.4 Consent In the GDPR, consent constitutes one of the assumptions for which data processing is considered legitimate. This means that although it is one of the most important features of the regulation, consent does not have a pre-eminence in the EU data protection system. Rather, it coexists with other legitimate assumptions established by law, namely: if necessary for the execution of a contract in which the data subject is a party; if necessary to fulfill a legal obligation of the data controller; if necessary to protect the vital interests of the data subject or other natural person; if necessary for the fulfillment of a mission in the public interest or in the exercise of public powers; and if necessary for the satisfaction of legitimate interests pursued by the data controller or a third party, as long as it those interests do not prevail over the interests or rights of the data subject.

On the contrary, in Argentine legislation, consent is the general rule for the legality of all personal data processing, and cases in which consent is not required are configured as exceptions to that

²⁵ Comparative table of own elaboration.

²⁶ See <http://registronacional.com/mexico/registro-nacional-de-proteccion-de-datos.htm>

²⁷ Comparative table of own elaboration.

rule. The Argentine law establishes as a general rule that all data processing must be done with the free, express, and informed consent of the data subject; according to these circumstances, consent must be made in writing or by equivalently explicit means. Thus, tacit or presumed consent is not considered valid by law, although such a rule has exceptions.

For its part, Chilean law provides that the consent of the data subject is necessary for the processing of their data, unless a legal provision has authorized it. The regulations establish that the consent should be express, informed, and in writing; and also contains cases where consent is excepted.

In Mexico, as a general rule, personal data may only be processed with the consent of the owner, obtained in a free, specific and informed manner. The consent must be express if the relevant data is personally sensitive, or pertains to finances or property holdings.

In Brazil several sectoral provisions require the express consent of the data subject. This arises from the General Telecommunications Law, the Consumer Protection Code and the Civil Internet Framework.

When defining consent, the Regulation states that "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her". Thus, European legislation does not use the term "express" in the legislation under consideration and admits that in addition to a declaration or statement, the presence of other "clear affirmative actions" are an expression of the consent of the data subject.

All legislation provides for various ways to revoke consent.

It is interesting to bring a point highlighted by our colleagues in Brazil in their report on the "legitimate interest" contained in European legislation (see above), since it has been the subject of special discussion in the legislative process concerning bill 5276/2016. Under this legal distinction, consent is still required, as long as it is free, informed and unequivocal. At the same time, this project included another hypothesis regarding the legal definition of the "legitimate interest" of the data controller. This hypothesis asserts that the terms means that there exist certain situations in which the explicit consent of the data subject is not considered necessary. In other words, if the data controller has a "legitimate interest" in the processing of the information, it would not be necessary to obtain the consent of the data subject.

This provision aroused the concern of various actors in Brazil since, on one hand, this definition means that parties other than the data subject may have legitimate interests in the processing, use, or transfer of given data. Furthermore, it allows circumstances to arise in which it is not possible to obtain the consent of the data subject, and/or in which the exercise of rights and the prevention of damages depend on the specific processing of the data in question.

But, on the other hand, InternetLab also emphasized that "legitimate interest" can be interpreted as an exception that allows a general authorization for all types of processing with any type of purpose,

without any control or knowledge on the part of the data subject. It was therefore emphasized that in order to establish an adequate balance between privacy protection and economic development, the government should set very clear limits for the use of “legitimate interest” as a legal basis for data processing in order to avoid abuses.

ii.5 Data subject’s rights Argentina, Chile, and Mexico contemplate in their legislations the famous ARCO rights, which consist of:

- Access: require the head of a database to provide information about the data relating to the person on the database, such as the origin and destination, the purpose of storage, who receives the data;
- Rectification: ask the head of a database to correct, update or modify the data if they are inaccurate, erroneous, misleading or incomplete.
- Cancellation: request the removal of the data when the storage lacks the legal basis or the data is out of date.
- Objection: request removal or blocking when a data has been voluntarily provided, or used for commercial communications and it is not desired to continue to be included in said database (see Chilean legislation).

The exercise of these rights does have exceptions, such as those established by the Argentine legislation regarding deletion or cancellation, which can not be done when doing so might affect rights or interests of third parties, or when there is a legal provision to keep the data. Brazil’s legislation also contains provisions relating to these rights, and circumscribes them to the areas of application of such rules. Thus, for example, the Brazilian Consumer Protection Code enshrines rights to access, rectification and cancellation.

The GDPR establishes traditional rights related to the protection of personal data, such as the rights to information, access, rectification, and objection. However, it adds other rights to the normative networks under analysis (except in cases which will be expressly indicated).

- Right to erasure or "right to be forgotten", by which every person has the power to request the deletion of personal data that are no longer necessary for the fulfillment of the purposes for which they were collected, when consent has been withdrawn and there is no other legal basis for the processing of the same, when the processing has been done illicitly, etc. In such cases, the data controller shall take reasonable measures, taking into account the available technology and the cost of its implementation, including technical measures, with a view to informing other data controllers for the request to delete any link to such personal data or any copy or replica thereof.

- Right to limit processing. By virtue of this right, the person may request that their data be preserved but no other type of processing be done. The conditions in which this right applies are: the data subject challenges the accuracy of the personal data, during a period that allows the data controller to verify the accuracy of the same; the processing is unlawful and the data subject does not request the suppression but its limitation; the data controller no longer needs the personal data but the data subject does for the formulation, exercise or defense of claims; or when the data subject has objected to a processing of data, while verifying whether or not the motive of the data controller prevails over those of the data subject. In these cases, the data subject can temporarily transfer the selected data to another processing system, prevent users from accessing the selected personal data or temporarily remove the published data from an Internet site.
- The right to portability, under which every person has the right to request data which they provided to a data controller for processing and to transfer them to another data controller, without the first data controller one being able to prevent it. The data subject can request the transfer of their data via whatever method is technically possible. Mexico contains a provision for data portability when dealing with public bodies.
- Right to object and direct marketing. In item 47 of section I, the Regulation maintains that “The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest”. However, the legislature has considered the right to the object the case of these databases to be a special case. In this sense, the granting of the right to individuals is always opposed to the processing of personal data which concerns them, including the creation of profiles. If the data subject exercises this right, data processing must cease for these purposes. In order to facilitate this exercise, the data controller is obligated to inform the data subject in the first communication of the existence of this right in a clear form and unrelated to any other type of information. Chile has a similar provision in its regulations.
- Individual automated decisions (art.22): The GDPR enshrines everyone’s right to not be the subject of a decision based solely on automated processing, including profiling, which produces legal effects on them, or significantly affects them in a similar way. In this way, the aim is to ensure a fair and transparent processing of the data subject in order to avoid — for example — decisions made by the use of algorithms that may exacerbate existing social patterns of discrimination and exclusion. Argentina and Mexico have similar provisions, applicable to the processing carried out by public bodies.

In relation to this last right included in European legislation, legal doctrines²⁸ have argued that in this case two rights can be derived from the Regulation. The first is the right to non-discrimination,

²⁸See Bryce Goodman and Seth Flaxman “European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation” 2016, Oxford, available at <https://arxiv.org/pdf/1606.08813v3.pdf>

whereby people have the right not to be discriminated against by algorithmic decisions based on the use of data that reveal racial, social, gender or other prejudices. The second is the right to an explanation, which empowers individuals to ask the data controller to report on the logic and operation of the algorithm used for their operations. As the name indicates, this right is satisfied when the process is explained in a clear and comprehensive way so that the data subject can evaluate if the decision has affected any of their rights.

It is worth adding that Brazilian bill 5276/2016 contains provisions regarding traditional ARCO rights for the data subject, as well as provisions in line with the GDPR.

ii.6 Responsibilities and obligations of those who process the data and the related subjects Parts of the legislation in the countries under study, as in GDPR, oblige the the data controller to adopt a series of measures in their data processing. It should be clarified that only one term has been used — data controller — but what is expressed must be extended to all subjects involved in data processing, as established by each particular legislation.

Among said measures, the following should be mentioned:

- Implementation of administrative, physical, technical and legal security measures for the processing and protection of data in order to protect against damage, loss, alteration, destruction; or its unauthorized use, access or processing, as well as guarantee its confidentiality, integrity and availability.
- Best practices scheme to raise the level of protection, harmonize processing, training, etc.
- Impact assessment in the protection of personal data, in order to assess the real impacts of a certain processing of personal data, in order to identify and mitigate possible risks.
- Notification of the owner and/or the enforcement authority in case of violation of data.
- Verification procedure to monitor and verify compliance with data protection provisions.

Obligations/responsibilities	Argentina	Chile	México	Brasil
Adoption of technical measures	+	-	+	-
Impact Assessment	-	-	+	-
Notification for breach	-	-	+	-
Verification procedure	-	-	+	-
Best practice scheme	-	-	+	-

Table 5.5.- Comparison of obligations and responsibilities.²⁹

²⁹Comparative table of own elaboration.

The GDPR adds a specific series of measures to be adopted, absent in the legislation under analysis, with the exception of Mexico in some cases. They are:

- Registration of processing activities to be carried out by each data controller.
- Privacy by design and privacy by default. The first consists of the obligation of all controllers to apply all necessary measures (pseudonymization, limitation of processing, etc.) to respect the privacy of users as the means of processing are determined. In this way, every service provider, software application or similar endeavor must take into account when designing a product that it does not affect the enumerated rights. Linked with this is the duty to guarantee by default that all data processing has only the objectives necessary for the purposes of its activity (privacy by default). These measures must also ensure that personal data are not accessible to an indeterminate number of people.
- Notification of a security breach.
- Impact assessment in data protection.
- Data Protection Officer.

ii.7 International data transfer References to these figures are found in Mexican legislation and in Argentine legislation.

In Mexican law, the transfer of the data to third parties or foreigners, other than the person in charge, will be done as agreed upon in the privacy notice, which will contain a clause stating whether or not the data subject accepts the transfer of data; in the same way, the third party who receives the data will assume the same obligations as the person or organization which transferred the data.

The law that affects the Mexican public sector establishes that any transfer is reliant upon the consent of the data subject and will be formalized by means of legal instruments which reveal the scope of personal data processing, as well as the obligations and responsibilities assumed by the original parties.

In Argentina the transfer of personal data from one base to another is allowed only if the following requirements are met: the assignment has been made to fulfill purposes directly related to the legitimate interest of assignor and assignee; the data subject has given their prior consent and they have been informed of the purpose of the assignment and of the identification of the assignee or of the elements in order to do so. If the transfer occurs, the assignee will be subject to the same regulatory and legal obligations of the transferor, which in turn must respond jointly to any violation of the law. Likewise, consent is revocable and the data subject may at any time request the transferee to stop processing their data.

However, Argentine law states that consent to the assignment or transfer is not always necessary. There are several exceptions to this rule: when a law provides consent or when it is one of the cases specified by the law in which consent to data processing is not necessary, such as the case of transfers of data directly between government agencies, provided that they are carried out within the framework of their competences; health data, provided that such data are necessary for public health, emergency or epidemiological purposes, and that the identity of the data subjects is preserved; and when a process of decoupling the information had been applied, so that people cannot be identified.

For its part, both the GDPR and the Argentine law support the principle that international data transfers are only allowed to countries with an adequate level of protection. When determining the criteria by which a country or organization is considered to have an appropriate level, the Regulation contains a detailed statement of the elements to be analyzed. These include: the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities, international commitments, etc. On the contrary, the Argentine law does not contain a similar level of specification. This omission was mitigated by a regulatory decree which established that the following should be taken into account: the nature of the data; the purpose and duration of the intended processing; the final destination of the data; legal, general or sectoral rules in force in the country concerned; professional standards, codes of conduct and security measures in place in those places; the destination's level of conformity with international or supranational organizations and regulations.

In the event that the country or organization does not meet these requirements, the GDPR limits transfers of personal data to cases in which the data controller or person in charge offers adequate guarantees, which can include: a legally binding and enforceable instrument between the authorities or public bodies, binding corporate rules, standard data protection clauses adopted by the European Commission or by a supervisory authority, a code of conduct or certification mechanism, etc.

If the data transferee cannot meet these requirements, the GDPR establishes a final list of assumptions in which the transfer proceeds, namely: when the data subject (owner) explicitly gave their consent; when the transfer is necessary for the execution of a contract between the data subject and the controller or the execution of a contract in the interests of the data subject between the controller and another natural or legal person; for important reasons of public interest; the formulation, exercise or defense of claims; or to protect the vital interests of the person concerned or other persons.

Unlike the GDPR, Argentine legislation provides for a short list of exceptions: international judicial collaboration; exchange of medical data when required for the treatment of the affected person or an epidemiological investigation; Bank or stock exchange transfers where the transfer has been agreed in the framework of international treaties to which Argentina is a party; or where the transfer is for international cooperation between intelligence agencies in the fight against organized crime,

terrorism and drug trafficking. In turn, the regulatory decree added the express consent of the data subject, and data contained in public records open to consultation by the general public.

ii.8 Application and enforcement mechanisms This section will analyze the mechanisms contained in the legislation under analysis to ensure the effective application and enforcement of the guarantees and protections contained in their provisions. To this end, four aspects will be addressed: (a) the enforcement authority and comptroller; (b) sanctions; (c) actions and remedies; and (d) compensation.

ii.8.1 Enforcement and controller authority The European regulations clearly established the guidelines with which the state enforcement authority and comptroller must comply. It should be clarified that the GDPR is not applied directly, but rather that it is the EU Member States which are charged with implementing the provisions of the community standard through their internal legislation.

In short, the GDPR indicates that the enforcement and control authority must have functional and financial independence in order to be able to freely carry out the corresponding controls over the processing of data by the government and by private organizations. The GDPR also requires certain qualifications and establishes conditions for the transparent designation and termination of the mandate of the head of the enforcement and oversight body. This is done in order to prevent the appointment and dismissal of the enforcement agency or enforcement agency director from becoming discretionary decisions made by the government in power.

In turn, the GDPR establishes that the enforcement body must have investigative, rectification, and consultation powers, must in all cases respect effective judicial review and protection after the fact, and must respect procedural safeguards. The power to initiate legal proceedings will depend on the specific internal legislation of each EU Member State.

In Argentina, the National Directorate for the Protection of Personal Data is a body under the Secretariat for Registry Affairs of the Ministry of Justice, and therefore it is dependent on the Executive Branch and, consequently, both the appointment and removal of its Director are subject to the discretion of the President. For this reason, and despite having among its powers the ability to control database processing by the government, it is compromised by the condition of dependence. The regulatory decree established as a requirement for the selection of the director to have “antecedents in the matter”, without establishing further clarifications and leaving, therefore, at the discretion of the Executive Power the determination and weighting of such antecedents. Although the regulatory decree establishes that the Directorate will maintain its independence, it lacks financial control. The Directorate has powers of investigation, sanction, and consultation, as well as being responsible for registering the bases for both the public and private sectors.

In the Chilean regulations, the data protection law does not explicitly refer to an institution that ensures compliance with the rule. In this way, individuals have been deprived of an authority to enforce compliance with the provisions of the law. The lack of institutionality allows data owners to turn to only to the police should they be affected by unauthorized processing of their data. It should be noted that for the public sector the following situation has occurred: Law 20.285 on Access to Public Information created the Council for Transparency, which among its main functions is to ensure compliance with the Law on Access to Information. However, it was also entrusted with "ensuring the proper compliance with Law 19.628 on the protection of personal data by the organs of the State Administration" (article 33). This has generated a situation in which certain experts declare that the law delegated the controller of data protection of public databases in the Transparency Council but with great doubt as to the scope of their faculties,³⁰ while others say that the interference of the Council for Transparency in the matter of personal data processing is indirect, since it only provides guidelines in order to limit state intervention — when it is a part of the state administration that performs personal data processing — or when it must resolve complaints in requests for access to public information that contains personal data, in accordance with legal regulations, without taking on an active role in the defense and promotion of the protection of the same.³¹

The Mexican legislation is clearer. It delegates enforcement to the National Institute for Transparency, Access to Information and Protection of Personal Data, which is the autonomous and independent body that is in charge of the application and control of data regulations both for the public sector and the private sector and which also has extensive powers of investigation, sanction, consultation, etc. The Mexican legislation finds itself strongly aligned with the GDPR.

In Brazil, given the lack of a comprehensive law on the protection of personal data, only the sectoral laws can be investigated, and so reiterate what is stated in section 5.2.2.i. when this document made reference to the fact that the Consumer Defense Code contains provisions regarding the protection of data applicable to consumer databases. For this purpose and in the specific area of its responsibility, it can be inferred that the National Consumer Directorate Under the Ministry of Justice acts as an enforcement body.

ii.8.2 Sanctions European legislation provides for two types of sanctions: economic and corrective. Economic fines must be imposed individually in an effective, proportionate and dissuasive manner, and the amount of the penalty should be adjusted according to the circumstances of the case. The elements to be taken into account include: the nature, severity and duration of the infringement, the intentionality or negligence of the infringement, the measures taken to remedy

³⁰ See item 3.1.2. in the Chilean report mentioned in section 5.2.2. of this document.

³¹ See: Álvarez Valenzuela, Daniel. "Acceso a la información pública y protección de datos personales: ¿Puede el Consejo para la Transparencia ser la autoridad de contralor para la protección de Datos". Revista del Derecho, Universidad Católica del Norte. Vol. 23 N° 1 Coquimbo, June 2016. Accessible at <http://bit.ly/2kRBUX5>

the situation, etc. The amounts of the fines vary according to the seriousness of the infringement and range from a fixed amount (up to €10,000,000 or €20,000,000 depending on the infringement) to a percentage (in the case of a company) of 4% of the total annual global business of the previous financial year. Criminal sanctions are decided by individual EU member states in their own jurisdictions.

In parallel, the GDPR provides that the control authority of each country may impose corrective measures jointly or in substitution of the fine. These measures may consist of warnings, warnings, limitation orders, rectification or deletion, withdrawal of certification, etc.

The laws of Argentina and Mexico are the only ones that contain provisions in this sense, while establishing economic and corrective sanctions. In addition they include the consecration of penal figures for cases of non-compliance.

ii.8.3 Actions and resources The GDPR grants the data subject the right to appear before the enforcement authority if the data subject believes that the processing of their data infringes the Regulation. The Regulation also grants them the right to appeal before the courts to request effective judicial protection in case the rights granted by the GDPR have been violated as a result of a processing of their personal data. The type of procedure will depend on the procedural legislation of each EU Member State.

Argentine law gives the data subject the possibility to appear before the enforcement authority to report breaches in the processing of their personal data. The law also contains provisions relating to the judicial procedure of habeas data, which gave content to and deepened the constitutional consecration of this right. The Argentine legislation ordered that the habeas data be governed by the rules of protection and, in supplementary form, by summary trial.

In the case of Chile, since there is no enforcement authority, the data owner does not have means to report a breach. The legislation only provides for habeas data judicial action, which must be filed before ordinary courts of justice. Mexico provides for a system which allows the data subject to make claims to the enforcement body for non-compliance with data protection regulations, which in this regard has quasi-judisdictional powers. Thus, Mexico stipulates various procedures and resources, including the reconciliation between the data controller and the data subject. These stipulations state that the comptroller body will resolve the differences between the two parties and that the possibility of resorting to judicial review will only be to challenge the ruling of the enforcement body. Because of this, Mexican law does not have a *habeas data* judicial procedure.

ii.8.4 Compensation (damages) The GDPR expressly establishes the right of all data subjects to claim compensation for material and non-pecuniary damages suffered as a result of an infraction by the data controller.

There is no similar provision in the Argentine law, in which the action of habeas data allows the person concerned to know the personal data stored or require their rectification, suppression, confidentiality or updating. No compensation is regulated for damages suffered. Although Law 25.326 mentions in Article 31 that database controllers are subject to liability for damages arising from non-compliance with their provisions, the right of data subjects to claim said compensation is not expressly enshrined, and as such the subject should refer any claim to the general rules of civil law.

Chilean regulations stipulate that the controller must compensate for damages. It is worth repeating here what our Chilean colleagues emphasize in their report:

"In addition to the comments on the disincentives that exist for action in ordinary courts, Article 23 also adds other questions. The first paragraph considers that in order to prosecute the responsibility of the data controller in case of undue data processing, the subject or prosecutor must prove the moral and property damage suffered as a result of said processing. In practice, it is difficult to know who has the data of the subject and what the controller does with them because, as we have seen, the mere fact of exercising ARCO rights in the Chilean context is already quite complex. Given this situation, it is unlikely that a data subject will actually know where their data are and what is being done with them, especially considering the absence of a control authority to ensure compliance with the regulations. Therefore, it is possible that the subject can only learn of the harm caused by undue processing with a wide temporal difference in judicial authorization."³²

The Mexican data protection regulations do not contain specific provisions regarding compensation for damages, but do contain general references to civil law.

Enforcement tools, available in data protection legislation	Argentina	Chile	México	Brasil
Enforcement and controller authority				
Dedicated exclusively	+	-	+	-
Functional independence	-	-	+	-
Public and independent annual budget	-	-	+	-
With powers of investigation and sanction	+	-	+	-
Sanctions				
Economic	+	-	+	-
Corrective	+	-	+	-
Criminal	+	-	+	-
AData subject's actions under a breach of data protection law				
Action before the enforcement authority	+	-	+	-
Judicial action (habeas data)	+	+	-	-
Compensation (legal claim for damages)	-	+	-	-

Table 5.6.- Comparison of Enforcement Tools.³³

³² See Chilean Report mentioned in section 5.5.2. page 9.

³³ Comparative table of own elaboration.

VI Conclusions and recommendations

Personal data has a transcendental role in the contemporary context. Its current place in our society is due to the profound changes that have taken place in the technological environment and the transformations that such a change has caused in the practices of companies and in their business models, in the organizational changes of the state, and in modifying the online behavior of individuals. The substantial increase in cross-border flows motivated by greater economic and social integration and greater exchange between public and private operators, in addition to the notable growth in the digital economy has created a scenario in which all these factors interact to such an extent that sometimes it becomes difficult to establish the boundaries between them.

More and more people's data are collected, stored and processed in all manner of ways, generating new data from that processing, of which the original data subject is not even aware. Beyond data or content that the data subject generates consciously, they also generate data with each movement that they perform online (metadata), which is generally unknown and beyond the data subject's control.

It is in this complex and quickly changing environment which the right to economic and technological development of peoples, free initiative and freedom of competition, the right to freedom of expression, of communication and of opinion, the right to private life, honor and image, the right of access to information, and the right to informational self-determination all come together.

To this we add the phenomena of big data (as a generic name for everything that refers to huge amounts of data and data processing) and automated decision making through the use of algorithms. In response to the development of these technologies, and with the purpose of mitigating the effects of "the black box" (referring to the algorithms which are not accessible because of issues related to intellectual or private property, or because they escape the understanding of the majority of the population), policy-makers have sought to establish a right to transparency and a right to an explanation of the criteria upon which the decision is based, both in concurrence with the right to non-discrimination.

The personal data and the information which can be generated from its use and processing puts the individual at the center of the scene. The tools for exercising the right to informational self-determination that the data protection laws of the 1990s developed may be insufficient in new contexts. Algorithmic decision-making, machine learning, and artificial intelligence leave little room to the individual for consent or control over their own information.

This is the setting in which various international bodies have begun to develop guidelines and principles aimed at strengthening the protection of privacy and personal data, while at the same time seeking to protect and balance the other rights which come together in this scheme. The General Data Protection Regulation in Europe is the most complete example of these efforts.

In the light of circumstances, concerns, and new dynamics, we must look at Latin America. The analysis of the data protection systems in four countries — Argentina, Chile, Brazil and Mexico — affirms that in general all of them have solid constitutional provisions which recognize the protection of privacy as a distinct legal right from that of informational self-determination. The regulation regimes also generally have specific regulatory provisions, although there are structural weaknesses in Chile's legislation, and Brazil stands as a significant exception, as it does not have a comprehensive data protection law.

The guiding principles in the processing of personal data are also consistent with those recognized internationally, although they do not refer to the principles of minimization or proactive responsibility. Consent plays a key role in the systems of the countries analyzed, without which the "legitimate interest" of the data controller would be sufficient for the processing of data, as it is in the European system.

The rights granted to data subjects by these national systems are consistent with the traditional protection, access, rectification, cancellation and objection line. Some of the legislation even contains provisions for newer tools, such as the right to portability and the right to a fair and transparent processing in the case of automated decisions.

The European legislation brings two novelties in this sense: the right to limit processing and the right to be forgotten — a name with which the right has wrongly transcended. This last right that the European Regulation recognizes is more akin to what the ADC prefers to call the "right to be removed from the index". This right has aroused heated discussions in numerous forums among those who argue that their adaptation would breach the right to freedom of expression and those who argue that it is an essential part of the right to informational self-determination. The tenor of this document does not allow us to delve into an analysis of these tensions, but they are being studied as well.

Of the systems studied, only the Mexican regulation is consistent with the standards set forth by the GDPR. The provisions relating to privacy by default and by design, notification in case of security breaches to the data subject and/or the enforcement authority, data protection delegate, and impact assessments are mostly absent from the Latin American systems analyzed.

The requirements for the assignment and international transfer of data are practically nil, with the exception of the Argentine legislation.

Finally, it should be noted that the enforcement tools, again with the exception of Mexico, are generally deficient. In Argentina, the weaknesses identified by the comptroller are incompatible with the actual exercise of the rights and guarantees established by the same law. In Mexico, the absence of habeas data has been referred to as a weakness, despite the multiple actions envisaged in the administrative process and the powers of the enforcement body. The situation is more serious in the case of Chile and Brazil, where there is a total absence of effective enforcement tools.

Thus, the study of these four countries shows that despite having apparently robust constitutional support, the scenario they generate in practice is characterized by its disparity and fragmentation, with structural weaknesses and a relative — or rather, negative — capacity of enforcement.

The study suggests the need to:

Strengthen the standards of protection of personal data and enforcement mechanisms.

Given the context described, the consideration and adoption of new provisions are necessary to strengthen the standards that are currently in place. We must discuss principles of minimization and proactive responsibility or the right to portability, as well as greater detail and feasibility analysis of concrete measures on the part of data controllers to ensure the best possible processing of personal data. The generation of more effective, clear, concise, and relevant channels of information for the individual, which enable the individual to fully understand the fate of their personal data, is still an outstanding issue.

Special attention should be given to the mechanisms and tools which enable effective implementation, enforcement, and protection, which have appeared as one of the main deficiencies in the regulations and are obstacles to the development of robust data protection systems.

Generate dynamic and inclusive mechanisms which allow us to identify and contain risks

generated by technological advances. The development of phenomena such as big data, the online market, algorithmic decision making, automatic learning, and artificial intelligence complicate elements of the data protection system, such as the notion of consent. Thus, legal tools such as the “legitimate interest” or the “compatible use of data” emerge which enable data processing facilities to act without the knowledge and consent of the data subject. Automated decision making and profiling by algorithms that few people know or understand paradoxically exclude their main protagonists. For proper identification, understanding, containment, and conciliation of these circumstances, and for the consequent generation of alternatives consistent with the right to informational self-determination, we must generate dynamic channels and mechanisms which include participation from stakeholders from the various sectors involved (data protection officials, private and technical sector, academia, and civil society).

Encourage instances of interaction and dialogue to strengthen informational self-determination

and its confluence with other human rights. The forcefulness of the right to informational self-determination, while guaranteeing the individual the control of their data, generates innumerable and permanent situations of conflict with other essential rights. Beyond the procedural and judicial channels, in which the conflicts in question will ultimately be solved, the generation of spaces for interaction and dialogue which allow the rigorous, expert, and permanent debate of the various confluences of the rights in question will enable expertise and

will strengthen the right to informational self-determination as an integral part of the human rights of the individual.

Move towards legislative harmonization. Rapid technological advances generate challenges that transcend geographical boundaries. The increase in the cross-border flow of data highlights the need to include legislative harmonization as an aspect of importance not only for the strengthening of data protection systems themselves but also for the development of the digital economy of the countries concerned and the region.

Pay special attention to particular situations. Although this work focused on general aspects of data protection systems, previous recommendations should also be considered, after study, in relation to special assumptions about data processing. Issues related to sensitive data, financial data, health data, data held by law enforcement and security authorities, to name a few, all come readily to mind. Likewise, data processing performed by the government requires special attention while enjoying significant exceptions.

We should add that the Ibero-American Network for the Protection of Personal Data appears as one of the leading forums for such dialogue and interaction since in addition to significant representation of data protection authorities from countries in the region and from international organizations, the Network boasts high participation from the private sector and academic observers, and, very recently, the participation of a representative for civil society. Of course, it would still be better for the mechanisms of participation to be more open.

Such forums notwithstanding, the process of legislative revision and reform in the selected countries is an opportunity to reflect on the various issues raised here and, if necessary, to take the appropriate measures.

Finally, it must be said that the reflections, conclusions and recommendations contained in this document are not finished and definitive positions, but instead are starting points for necessary dialogues, debates and interactions that are inescapable for the strengthening of human rights not only in Argentina, Chile, Brazil and Mexico, but throughout Latin America.

