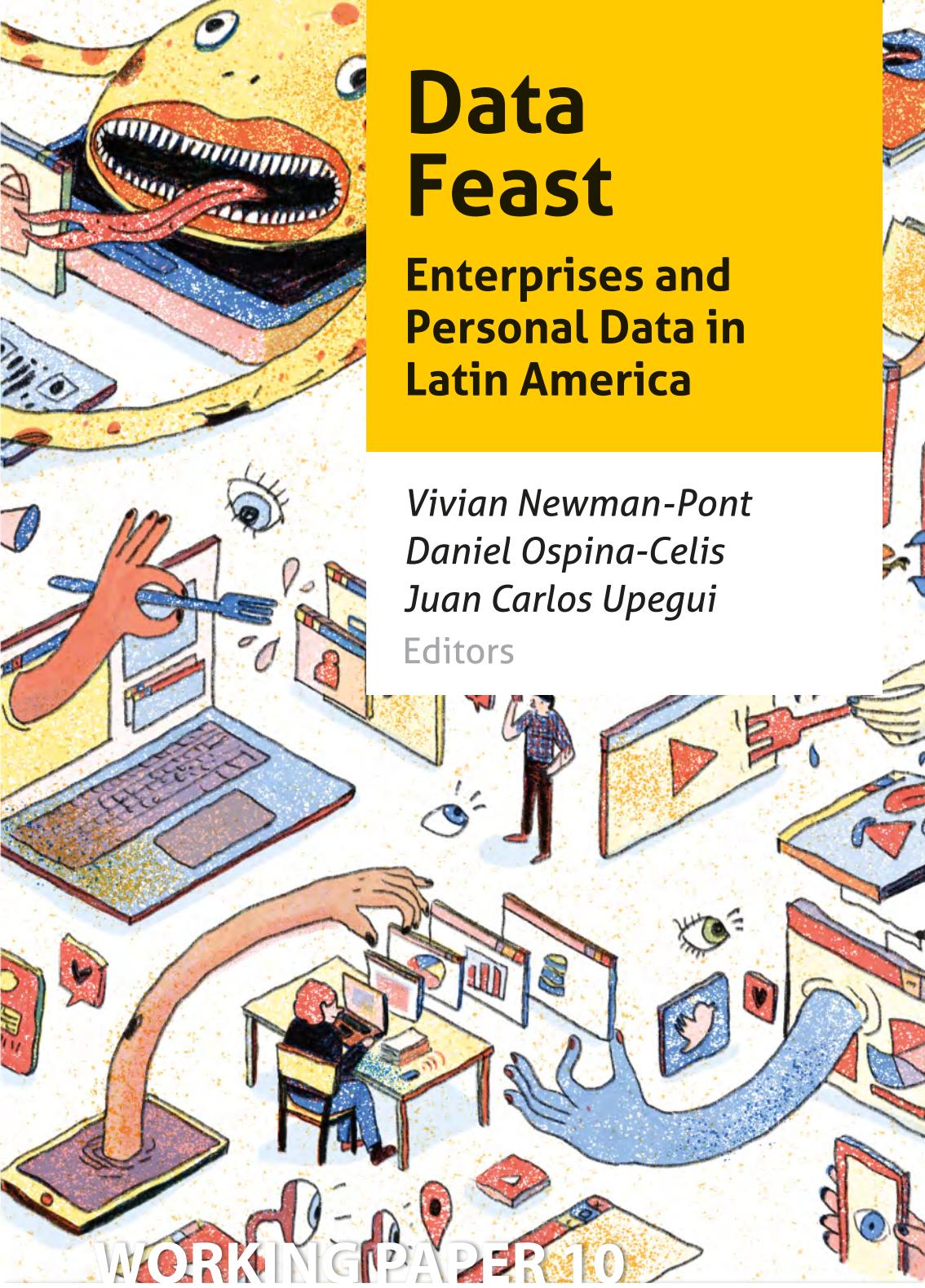

# Data Feast

## Enterprises and Personal Data in Latin America

*Vivian Newman-Pont*
*Daniel Ospina-Celis*
*Juan Carlos Upegui*
Editors

WORKING PAPER 10

Dejusticia

**Vivian Newman-Pont** obtained her law degree from the Universidad Javeriana and her Bachelor of Laws degree from the Universitat de Barcelona. Vivian holds a post-graduate degree in Administrative Law (D.S.U.), a Master's degree (D.E.A.) in Internal Public Law from the Université Paris ii Panthéon-Assasand, as well as a Master's degree in Cooperation and Development from the Universitat de Barcelona. She is the Director of Dejusticia.

**Daniel Ospina-Celis** is a lawyer who studied at the Universidad de los Andes and is a researcher for Dejusticia.

**Juan Carlos Upegui** is a lawyer and head professor at Universidad Externado de Colombia. He holds a PhD in Law from the Universidad Nacional Autónoma de México (UNAM). He is also a researcher for Dejusticia.

# Data Feast

## Enterprises and Personal Data in Latin America

*Vivian Newman-Pont,*
*Daniel Ospina-Celis, and*
*Juan Carlos Upegui*
Editors

Dejusticia
law · justice · society

Data Feast: Enterprises and Personal Data in Latin America

Vivian Newman-Pont, Daniel Ospina-Celis, and Juan Carlos Upegui, Editors
Data Feast. Enterprises and Personal Data in Latin America. — Bogota: Editorial Dejusticia, 2020.
196 pages: graphs; 24 cm. — (Working Paper; 10)
ISBN 978-958-5597-53-2
1. Personal data protection 2. Businesses and human rights 3. Privacy
4. Technology and human rights — Latin America I. Tit. II. Series.

**Working Paper 10**
DATA FEAST
Enterprises and Personal Data in Latin America

ISBN 978-958-5597-53-2 digital version

Dejusticia
Calle 35 No. 24-31, Bogotá D.C.
Telephone: (+57 1) 608 3605
info@dejusticia.org
https://www.dejusticia.org

This document is available at https://www.dejusticia.org



Translation: Carlos Alberto Arenas
Copy Editing: Ruth Bradley
Layout: Diego Alberto Valencia
Cover design: Alejandro Ospina

Bogotá, November 2020

## CONTENTS

## ACKNOWLEDGMENTS

This research is the result of the concurrence of many efforts, both individual and institutional.

First, we would like to thank our partners at Coding Rights in Brazil, Derechos Digitales in Chile, and Red en Defensa de los Derechos Digitales (R3D) in Mexico; especially the authors of the chapters per country: Joana Varon, Bruna Martins dos Santos, and Kimberly Anastácio (Brazil); Paloma Herrera and Pablo Viollier (Chile); and Milan Trnka Osorio (Mexico), and all the people who contributed their experience to refine the reports of their respective countries. Their dedicated work during the second half of 2019 gave us insight to compare countries, make final recommendations, and for the final consolidation of this book.

We would also like to thank our colleagues at Dejusticia for attending the discussion seminar and for their comments on the first draft of this book. Their feedback and recommendations improved the text. The support and guidance of Celso Bessa and Víctor Saavedra were also pivotal to alleviate the inaccuracies in the use of technical expressions. To María Paula Ángel who came up with the project and for her careful review of the chapter on Colombia and the comparative study. Similarly, we would like to thank Dejusticia's administrative team for their daily support and dedication. We especially thank Claudia Luque for her invaluable collaboration throughout the publishing process.

Similarly, we thank Alejandro Londoño and Sarah Osma of the Deputy Superintendence for the Protection of Personal Data; Jonathan Bock and Luisa Izasa of Fundación para la Libertad de Prensa; Lucía Camacho of Fundación Karisma; Ailidh Callander of Privacy International; and José Alejandro Bermúdez, consultant and expert, for attending our focus group and offering time, insight, and feedback on the draft. We also thank

Nelson Remolina, current Deputy Superintendent for Data Protection in Colombia, for his interest in this research and his readiness to share his opinions.

Finally, and with a special mention, we want to thank Wellspring, our international funder. Without its support, we would not have completed the comparative work, compilation, and final editing of this book.

# INTRODUCTION

*Daniel Ospina-Celis*
*Juan Carlos Upegui*

## 1. Digital Economy and Big Data

Technology in general, and information and communications technologies (ICTs) in particular, have changed our everyday life. Recent technological developments have driven paradigm changes in various areas of knowledge and our relationship with our environment. Easy access to mobile devices (smartphones, tablets, laptops, etc.) has changed how we interact with technology. According to a study by GSMA, a global association of mobile operators, by 2018 smartphones were used by 66% of the world's population and 85% of the Global North's population (GSMA 2018). We live in a technological society where the majority of the population uses a mobile device every single day.

Recent technological developments, the evolution of the Internet, and the interconnectivity of devices have led some to claim that we are undergoing a fourth industrial revolution. Considering the possibilities of the technification and digitalization for global trade, the German government introduced the Industry 4.0 initiative in 2011. The program aims to drive digital manufacturing forward by increasing digitalization and the interconnection of products, value chains, and business models. In the framework of this initiative, "Data-driven business models will become a major driving force of Industrie 4.0 in the future" (European Commission 2017, 7). Although the German program was ground-breaking at the time—so much so that today the term "Industry 4.0" is used in academia and business—by 2020, assuming that digitization and data are commonplace in modern society will no longer seem far-fetched.

This digital revolution is also characterized by using hybrid production systems ("cyber-physical systems") based on data and knowledge integration (Lu 2017). This practice facilitates meeting each user/customer's individual needs, creating a more efficient production system, improving the relationship between the end user and the producer or distributor, and integrating and automating the market (Vaidya, Ambad, and Bhosle 2018). The use of data plays a significant role in the fourth industrial revolution. As mentioned by the Boston Consulting Group, "The collection and comprehensive evaluation of data from many different sources" optimizes the production, saves energy, and will become standard to support real-time decision-making (2015, 5).

ICTs collect and create digital data thanks to the Internet, social media sites, mobile devices, applications downloaded on them, and many other digital interactions involving thousands of people every day. This data is of high value to anyone who can analyze it. From a person's data, you can infer, for instance, what kind of music they like, whether they have a newborn child, and even their political views. This information is commercially valuable because it allows companies to offer personalized advertising, just to mention one of its uses. For this reason, thousands of companies collect, process, analyze, or commercialize digital data. This is why some talk about an industrial revolution primarily based on the massive use of data.

The economic value of the data and the possibilities its correct use provides for the industry have led thousands of companies to seek access to this market. These enterprises have been called "companies with data-driven business models" (CDDBMs) because they collect or analyze data, sell data-based products or services as their primary activity, and/or rely on data as a critical resource in their business model (Hartmann et al. 2014, 6). Although there are several classifications of CDDBMs—depending, in part, on the specific use given to the data—the preponderance of third-party data processing in their commercial activities is common, whether for direct marketing, use in customer/user segmentation, service optimization, or customer loyalty.

The digital economy and the fourth industrial revolution revolve around the massive use and analysis of data. Big data becomes relevant in this context, understood as the "information assets characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value" (De Mauro, Greco,

and Grimaldi 2014, 8). The consensual definition of big data implies that data are analyzed by interlinking three elements: 1) the data variety, 2) their volume, and 3) the velocity at which information changes (Elgendy and Elragal 2014). However, this definition does not prevent some analysts from including additional elements such as the complexity of data (Pence 2014).

It is not in vain that data has been considered as one of the major assets of the 21st century economy, mainly thanks to the analysis big data allows. Among many other reasons, this is because, although data is attributable to individuals, a third party—usually a company—derives economic benefit from its exploitation by aggregating and analyzing it. As Michael Haupt (2016) said, data is a resource created by and for sovereign human beings; therefore, we cannot allow "a new breed of corporations to extract wealth from us, like we've allowed in the past" with other resources, without active participation from data subjects, appropriate regulation, and accountability practices for corporations that amass these data and, in so doing, increase their power.

Although the collection and analysis of digital data may seem distant, by downloading any application on a mobile device, the company that owns said application usually gains access to a large amount of data stored on our devices, as stipulated in its privacy policy. For example, the company may gain access to the photographs we have saved, our contacts, location data, basic information on the device, or even the remaining battery percentage. Thus,

> the development of the digital economy and big data pose significant challenges for the rights to privacy, the protection of personal data, equality, and transparency, and data security (Newman and Ángel 2019, 10).

It is necessary to mitigate the risks created by new personal data processing practices and the alternatives big data offer to ensure human rights in the digital world.[1]

The Article 29 Working Party, an initiative of the European Parliament working under the name of European Data Protection Board since 2018, has identified that the analysis of vast quantities of data (big data)

1. See Ana Beduschi (2019) to follow the discussion on the use of technology and big data to create digital identities and safeguard human rights.

raises concerns. For this group of experts, big data poses new challenges for the protection of privacy in the following issues: 1) the sheer scale of data collection and the possibility of profiling people with detail, 2) data security, 3) the transparency data processing systems require to allow individuals to understand and control the use of their information, 4) the possibility of being subjected to arbitrariness or unjustified discrimination, and 5) increased state surveillance, reflected in a massive control of information of all citizens (Article 29 Working Party 2013, 45).

Some technology enthusiasts claim that one of its most significant benefits is its full impartiality to people, which may lead to fairer resource distribution. While this may be true, big data and algorithms can often reproduce social biases and cause discrimination. Barocas and Selbst (2016) discuss how big data has a "disparate impact" on access to employment. Although very similar to discrimination, this impact differs because (at least in the authors' opinion), the intent to discriminate cannot be demonstrated.[2] Other authors have argued that some algorithms used to process personal data may be openly discriminatory if not used properly—i.e., if there is no full transparency in their design and application—and their risks are not mitigated (Kleinberg et al. 2018). For this reason, and to avoid injustices deriving from the inappropriate use of technology (especially artificial intelligence), the struggle for "algorithmic transparency" has gained strength in recent years.

Moreover, the collection of large amounts of data allows companies to profile people. These profiles are useful for CDDBMs insofar as they enable them to determine what products or services a group of people can access or what information to provide them. This generally depends on the "traits" extracted or derived from people's online behaviour. Profiling is usually carried out for commercial purposes, such as offering targeted advertisements according to individual tastes. However, its uses may be diversified to advance various ideological, political, religious, or commercial agendas. Profiling practices may cause discrimination—as only certain people may access certain content—and may also affect the right to freedom—by inducing particular behaviour and changing the online behaviour—and can have other impacts, as yet insufficiently explored, on people's behaviour and human rights.

2. This argument was adopted by Professor Frederik Zuiderveen Borgesius (2018) in his study for the Council of Europe (one of the largest human rights organizations on the continent).

## 2. The Issue of Regulation

The economic importance of using and analyzing data for the digital economy—nowadays, a transnational and global economy—is undeniable. The massive collection of personal data through the Internet and mobile devices is undeniable and poses significant risks for society and human rights in the digital age. Therefore, the personal data collection, use, analysis, and processing practices of CDDBMs must be regulated somehow to safeguard the rights to data protection, privacy, and equality, among others.

However, regulating the CDDBMs' processing of personal data in the digital scenario is no easy task. There are several reasons for this. First of all, due to the transnational commercial dynamics of large Internet companies such as Google, Amazon, Facebook, Apple, and Microsoft (GAFAM), data protection "is no longer a national topic," but must be seen as an issue that transcends borders (Culik 2018, 29). Second, due to their tremendous economic power. According to Fortune 500's website, the market value of Microsoft as of March 29, 2019, was close to US $900 billion.[3] This value far exceeds the GDP of several middle-income countries, such as Colombia. According to the World Bank, in 2018, its GDP was approximately US $330 billion;[4] almost a third of Microsoft's market value. Although this is an illustrative example, the economic imbalance between one actor and another makes the effective regulation of the commercial activity difficult. In Todorov's words, "Faced with the disproportionate economic power held by individuals or groups of individuals with immense capital at their disposal, [national] political power often turns out to be too weak" (2012, 94). Also, companies that are present in multiple countries must adopt a practice that is replicated at a global level (the processing of personal data) to the unique and specific legislation of each country, and not to a global or at least regional legislation—a phenomenon known as the problem of fragmentation. This situation makes it difficult for transnational CDDBMs to adapt their data processing practices to the specificities of the national legislation of the countries in which they operate.

3. Search results of Fortune's website: https://fortune.com/fortune500/2019/search/?mktval=desc&sector=Technology

4. Search results of World Bank's website: https://data.worldbank.org/country/colombia

On the other hand, the transnational nature of several CDDBMs means that holding them accountable at a national level is a challenge. Based on the traditional rules of territorial application of the law, the domestic legal system often does not recognize jurisdiction over the actions of companies domiciled in other countries. In turn, the latter are reluctant to respond in formally "extraterritorial" jurisdictions. As this book will present, the competence of national data protection authorities over the actions of companies processing data of its citizens, but whose parent company and/or effective domicile is in a different country—usually the Global North—is not entirely clear. In practice, CDDBMs resort to this argument when any administrative or judicial authority attempts to hold them accountable for their actions.[5]

Another reason why it is not easy to adequately regulate the processing of personal data by CDDBMs—or big data in general—is the technical complexity of the subject and, therefore, the high level of detail required for a satisfactory regulation. As shown in the subsequent chapters, issuing general rules on data protection is not enough in the digital age if these, or their interpretation, do not conform to the technical reality of big data and the various forms of data collection, use, and analysis that are possible thanks to computer systems. Thus, both the legislator and the interpreters of the law must address (and, ideally, know and understand) issues such as metadata collection, the use of cookies, the interoperability of systems and databases, automated decisions, and the data market.

## 3. Two Relevant Regulations: Europe and California

Considering the risks of mass collection and subsequent analysis of personal data in the digital age by CDDBMs, both the European Union and the State of California (United States) issued data protection regulations

5. In this regard, see the arguments of Google LLC and Google Colombia Ltda. in the motion to vacate ruling T-063A of 2017, whereby the Constitutional Court ordered the former to delete certain content from www.blogger.com. Here, Google LLC argued that the Constitutional Court of Colombia had no jurisdiction to order it to delete content, mainly because Google LLC had no physical domicile in Colombia, as it provides its services remotely via the Internet. Although the ruling was vacated through Writ 258 of 2018 and the case was finally solved through Ruling SU-420 of 2019, in the meantime, Google decided to comply with the legal order and deleted the blog that caused the controversy.

adjusted to the digital age. These regulations are worth mentioning because they aim to overcome some of the problems and/or limitations described in the preceding section and protect the rights of users of digital services or platforms.

On April 27, 2016, the European Parliament and the Council of the European Union adopted the General Data Protection Regulation (GDPR)—EU Regulation 2016/679 of the European Parliament and of the Council.[6] This Regulation became effective on May 25, 2018, and updated the European data protection regulations according to the dynamics of the digital age. The Regulation explicitly recognizes that "rapid technological developments and globalization have brought new challenges for the protection of personal data," insofar "the scale of the collection and sharing of personal data has increased significantly" (GDPR, Recital 6). It is important to note that the GDPR applies to the processing of EU residents' personal data, even if the controller (CDDBM) is domiciled outside of the EU, provided that the processing relates to the offer of goods and services (Article 3). It is also worth mentioning that the GDPR extensively regulates the consent given by the data subject—so much that it allows for its withdrawal—(Article 7) and grants the data subject rights such as the right to portability (Article 21) and the right to object (Article 21), while imposing strict transparency standards on the data processor (Articles 12 to 14).

The European regulation is relevant for our analysis for at least two reasons. First, because it is a regional regulation that seeks to balance the economic power of commercial operators that process personal data (CDDBMs) with the European Union's political power. In that sense, it has the potential to be complied with by the companies because it is not a country's isolated effort to regulate big data but of a group of nations that represent a significant part of the data market and the world's digital economy. Second, because the GDPR is aligned to the digital age's technical reality; it regulates aspects of data processing in the 21st century that other (earlier) regulations ignore. In any case, this does not mean that it is

6. European Union, General Data Protection Regulation (GDPR). European Parliament and Council Regulation EU 2016/679, "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC." April 27, 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

a regulation to be emulated verbatim by the Latin American States. However, the GDPR constitutes a reference or a baseline for the current and future national legislations of the countries in the region.

However, the territoriality of the data protection law and its scope concerning transnational companies is also an issue of interest at the European level. Recently, in September of 2019, the Court of Justice of the European Union established that the GDPR in no way mentions that "the rights enshrined in those provisions would go beyond the territory of the Member States." Therefore, the Court concludes that, according to the European regulations, Google cannot be obliged to de-reference content hosted in a national version of the search engine that is not a member of the European Union.[7]

On the other hand, in 2018, the State of California enacted Act AB-375, partly inspired by the GDPR. This act, also called the California Consumer Privacy Act (CCPA),[8] partially amends the Civil Code of California. This act became enforceable on January 1, 2020, and updated the state's data protection regime to the dynamics of the digital age recognizing, among other things, the consumers' right to know what personal information CDDBMs collect (Section 1.798.110) and to object to the sale of their personal data (Section 1.798.120).

Although it is not a countrywide regulation for the United States, the CCPA may have an impact similar to the GDPR because, being a regulation for the State of California, "Its large population and economy give its bills considerable influence in the rest of the country." (Newman and Ángel 2019, 13). Another element to remember is the fact that several of the world's big Internet companies are based in California. As an example, this implies that the CCPA has territorial application over CDDBMs like Facebook (based in Menlo Park, California), Google (based in Mountain View, California), Apple (based in Cupertino, California), Netflix

7. Court of Justice of the European Union, Judgment C-505/17. Reference for a preliminary ruling—Personal data—Protection of individuals with regard to the processing of such data—Directive 95/46/EC—Regulation (EU) 2016/679—Internet search engines—Processing of data on web pages—Territorial scope of the right to de-referencing. European Union: CVRIA. September 24, 2019, http://curia.europa.eu/juris/document/document.jsf?text&docid=218105&pageIndex=0&doclang=EN&mode=req&dir&occ=first&part=1&cid=166644

8. California Consumer Privacy Act (CCPA), 2018. Retrieved October 23, 2019, from https://oag.ca.gov/privacy/CCPA

(based in Los Gatos, California), and Twitter (based in San Francisco, California), to name a few.

## 4. Inputs for Regulation in Latin America

Although there is no binding international regulation on the protection of personal data at a regional level, two bodies have advanced these discussions. On the one hand, the institutional framework of the Organization of American States (OAS), under the instructions of the General Assembly, the Department of International Law, and the Inter-American Juridical Committee, consulted the Member States on the matter and prepared reports. On the other hand, the Ibero-American Data Protection Network comprises the data protection authorities of over 13 countries.[9] In 2017, this Network approved the *Standards for Data Protection for the Ibero-American States*. Despite being a soft law instrument, these Standards are relevant for at least two reasons: 1) because they serve as a benchmark for the States of the region, and 2) because one of its primary purposes is the processing of personal data in the digital age. This purpose is evident in Article 1, according to which the Standards seek to raise the protection level of individuals regarding the treatment of their personal data, which answers to the "needs and demands that the right to the protection of personal data demands in a society in which information and knowledge technology are increasingly relevant in all matters of daily life."

These Standards include clauses of great importance for the processing of personal data in the digital age. They include the extraterritorial application of its provisions when the data processor or controller is not domiciled within the territory of the Ibero-American countries. However, the processing activities are related to the offer of goods or services aimed at residents of the Ibero-American States (Article 5.1). Furthermore, it is an open-texture legal instrument due to the many principles it incorporates (Articles 10 to 23). Similarly, it recognizes the rights to access (Article 25), correction (Article 26), cancellation (Article 27), and objection, especially when data is processed for marketing or profiling (Article 28). Finally, we emphasize that the Standards ensure the right of

9. Ibero-American Data Protection Network, "Standards for Data Protection for the Ibero-American States," June 20, 2017. https://iapp.org/media/pdf/resource_center/Ibero-Am_standards.pdf