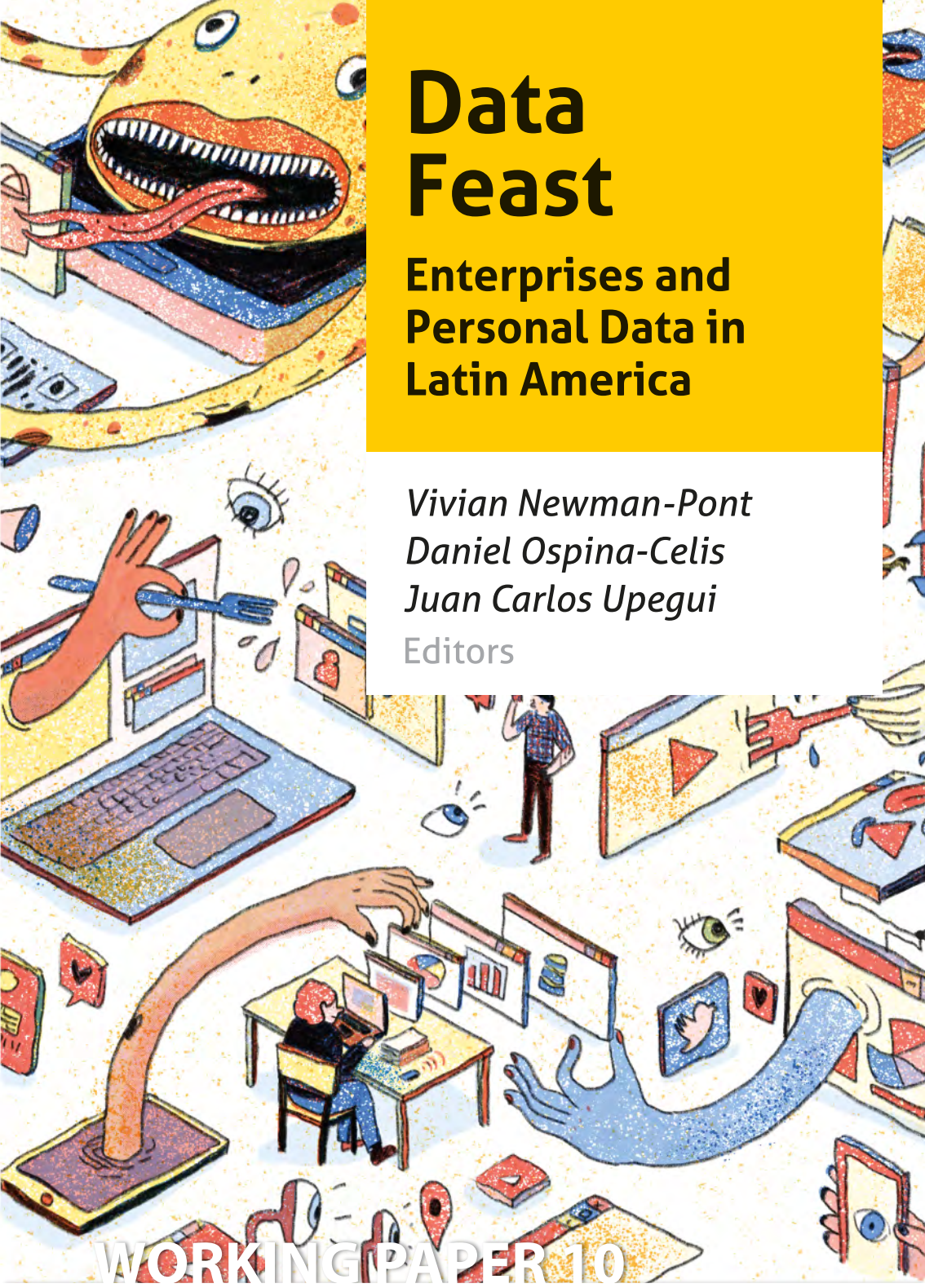


Data Feast

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 **9**

INTRODUCTION **11**

1. Digital Economy and Big Data 11
2. The Issue of Regulation 15
3. Two Relevant Regulations: Europe and California 16
4. Inputs for Regulation in Latin America 19
5. Book Methodology and Structure 20
6. Country Reports 21
7. Scope of the Research 23

References 23

APPLICATION OF THE PERSONAL DATA PROTECTION LAW IN BRAZIL: A CASE STUDY OF SOME DATA-DRIVEN BUSINESSES **26**

1. Selection of CDDBMs 27
2. Characterization of CDDBMs' Operations 31
3. Evaluation of the Personal Data Protection Legal Regime to Address the Dynamics of the Companies Analyzed 45
4. Evaluation of the National Data Protection Authority's Capacity to Deal with CDBBMs 59

Conclusion and Recommendations 63

References 66

ACCOUNTABILITY OF FACEBOOK AND OTHER BUSINESSES IN CHILE: PERSONAL DATA PROTECTION IN THE DIGITAL AGE 69

1. Methodology 70
2. Selection of CDDBMs 71
3. Characterization of CDDBMs Operations 75
4. Capacity of the Personal Data Protection Legal Regime 87
5. Evaluating the Capacities of the Data Protection Authorities 102

Conclusions and Recommendations 105

References 106

ACCOUNTABILITY OF COMPANIES WITH DATA-DRIVEN BUSINESS MODELS IN COLOMBIA: PERSONAL DATA PROTECTION IN THE DIGITAL AGE 111

1. Introduction and Selection of CDDBMs 111
2. Operations of CDDBMs Collecting Data in Colombia 114
3. How Prepared are the Colombian Personal Data Protection Regime and the Competent Authorities to Face the Challenges Posed by the Digital Age 117

References 131

ACCOUNTABILITY OF CDDBMs IN MEXICO 132

1. Selection of CDDBMs 132
2. Characterization of the CDDBMs' Operations 133
3. Evaluation of How Prepared the Personal Data Protection Legal Regime Is to Address the New Dynamics of the Digital Age 138
4. Evaluation of the Capacities of the Data Protection Authorities to Hold the CDDBMs Accountable 150

Recommendations 152

References 154

CDDBMs AND PERSONAL DATA PROTECTION IN BRAZIL, CHILE, COLOMBIA, AND MEXICO: THE COMMON EXPERIENCE 157

1. Standard Aspects and Risks of CDDBMs Operations 161

2. Data Protection Laws in Brazil, Chile, Colombia, and Mexico 174

Conclusions and Recommendations 184

References 189

ABOUT THE AUTHORS 191

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

individuals not to be subject to automated decisions that cause them legal effects or similar without human intervention (Article 29).

5. Book Methodology and Structure

This book stems from the question on the suitability of the data protection regulation in four Latin American countries—Brazil, Chile, Colombia, and Mexico—to face the challenges of data processing in the digital age and the existence of mechanisms to hold CDDBMs accountable. This question includes other, more specific, questions on the CDDBMs' data processing practices, the mechanisms available to the national data protection bodies to ensure the rights of data subjects, and the need (or not) for a regional—Latin American—personal data protection regulation in the digital age.

We chose four Latin American countries (Brazil, Chile, Mexico, and Colombia) for a combination of practical reasons and because they are representative of what is happening in the region. The practical reasons range from the location of Dejusticia's headquarters, the organization that hosted the project (Colombia), to the existence of friendly and trusting relationships with other organizations working on digital rights and data protection in the region. Coding Rights, an organization working on human rights and the use of technologies from a feminist perspective, is based in Brazil. Derechos Digitales, which has been studying the subject for over 15 years, is based in Chile. Finally, Red en Defensa de los Derechos Digitales (R3D), an organization specializing in the use of data in the digital age, is based in Mexico.

Furthermore, we believe that these four countries are representative to present a modest overview of the phenomenon in the region. This selection combines several factors: their varied geographic location, the size of their population, the use of Spanish and Portuguese as official languages, their relative regulatory and institutional development on the matter, and, finally, the size of their economy. We consider this last point relevant because it serves as an incentive for transnational CDDBMs that have a presence, or seek to intensify it, outside the domicile of their parent companies.

To solve the questions that guide this research, we slightly readapted the methodology used in Newman and Angel's previous work *Accountability of Google and Other Businesses in Colombia: Personal Data Protection in the Digital Age* published by Dejusticia in 2019. For each

country, we identified four CDDBMs in each of the following categories: 1) large Internet companies, known for their extensive investment capital (GAFAM); 2) intermediate companies, which are under consolidation, but not yet at the level of large Internet companies; 3) start-ups, known for their young age and large capacity for growth; and 4) established companies, which are businesses preceding the digital revolution and have adjusted their business model to the digital age.

After identifying the CDDBMs, the data processing policies of their most relevant products are analyzed to characterize their way of operating regarding the following issues: 1) data sources, 2) processing, 3) purpose of data processing, and 4) relationship with GAFAM. Then, the authors evaluate: 1) how prepared is the data protection legal regime to deal with the dynamics of the digital age, as opposed to the corporate practices identified above, and 2) the capacity of the national data protection authority—or, in its absence, judges—to hold CDDBMs accountable, taking into account their monitoring, control, and/or enforcement duties. Finally, the authors make recommendations based on the findings and the case analysis.

The process of writing the results of the research also involved a focus group in each country (Brazil, Chile, and Mexico) with experts on data protection, human rights defenders, and members of academia and industry representatives.

After receiving the country reports, these were compared to prepare a sort of regional compilation report. This comparison, included as the final chapter of this book, contains an overview of each country's main findings in the points mentioned in the methodology that guides the production of country reports and seeks to emphasize the patterns or common findings that guide the final recommendations.

Finally, the compilation work, which includes this introduction, the country reports, and the comparative study, were submitted for review and comments from the authors of the country reports, various actors of the industry, and experts on the subject during a focus group held on February 20, 2020, at Dejusticia headquarters in Bogotá, Colombia.

6. Country Reports

Following the methodology mentioned above, in Chapter 1, Kimberly Anastácio, Bruna Martins dos Santos, and Joana Varon analyze the Brazilian legal regime (emphasizing on the recently enacted Law 13.709

of 2018)[10] in the light of the personal data use practises of four CDDBMs operating in Brazil: Amazon, iFood, Social Miner, and Magazine Luiza.

In Chapter 2, Paloma Herrera and Pablo Viollier analyze how Facebook, PedidosYa, AIRA, and Falabella operate in Chile. Their text also compares the provisions of Law N° 19.628 on the protection of privacy with the bill that "regulates the protection and processing of personal data and creates the Personal Data Protection Agency," being discussed by the National Congress of Chile as of the writing of this publication (February 2020).

In Chapter 3, Maria Paula Ángel-Arango, Vivian Newman-Pont, and Daniel Ospina-Celis present an updated summary of their research, previously published under the title *Accountability of Google and other Businesses in Colombia: Personal Data Protection in the Digital Age*. Unlike the chapters for Brazil, Chile, and Mexico, this text analyzes the terms of service of thirty CDDBMs operating in Colombia, along with the provisions of Law 1581 of 2012[11] and the capacity of Colombia's data protection authority to hold CDDBMs accountable.

In Chapter 4, Milan Trnka Osorio analyzes Mexico's data protection regime and the role of the National Institute for Transparency, Access to Information and Personal Data (INAI, for its acronym in Spanish) as the data protection authority. This text emerges from the privacy policies of Amazon, Snap Inc. (Snapchat's owner), Payclip S. de R. L. de CV, and Radio Móvil Dipsa S. A. De C.V. (Telcel's owner).

Finally, Chapter 5 contains an analysis by Daniel Ospina-Celis and Juan Carlos Upegui. Based on the country studies mentioned above, they compare the legal regimes and the commercial practices of the companies studied in Brazil, Chile, Colombia, and Mexico. This chapter seeks to establish the common ground between the research results in each country to determine the shared challenges—regarding corporate practices—and the shared needs for regulation—regarding the scope of the national laws or the capacity of the data protection authority.

---

10. Government of Brazil, "Lei Geral de Proteção de Dados Pessoais" [LGPD; Personal Data Protection Law]. Law 13.709, August 14, 2018. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

11. Statutory Law 1581 of 2012, "Whereby general provisions for the protection of personal data are issued." October 18, 2012, D.O. 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

7. Scope of the Research

Due to the methodology described above and the selection of only four Latin American countries as the object of study, this research is limited in scope. The analysis of how CDDBMs collect and analyze personal data was mainly based on a thorough reading of their products' privacy policies. This research was not based on a technical study of the data collection and analysis technologies each company uses, or on an empirical study that uses qualitative or quantitative methodologies to collect and analyze information. This implies that, should there be differences between what the companies concede in their privacy policies and their actual actions, the latter are beyond the scope of this research. Furthermore, this book's limited scope is compounded by the lack of transparency and thoroughness in the privacy policies studied.

On the other hand, although the CDDBMs studied in each country belong to a broad spectrum of companies—due to their varied size and economic power—they are far from being a statistically representative sample of all the companies with data-driven business models operating in each territory. This study does not intend to be statistically significant. Rather, the companies selected show that it is likely that the personal data processing practices are similar (with some nuances) across companies in the digital economy. This also applies to the four countries studied. Even if this is a representative number of Latin American countries, the findings described here do not allow us to conclude that the results of this research may be extended, without nuances, to the other countries of the region.

REFERENCES

Article 29 Working Party. 2013. Opinion 03/2013 on purpose limitation. Adopted April 2, 2013, 00569/13/ENWP203, 45. https://ec.europa.eu/justice/article-29/documentation/opinion-ecommendation/files/2013/wp203_en.pdf

Barocas, Solon, and Andrew Selbst. 2016. "Big Data's Disparate Impact." *California Law Review 104*: 671–732.

Beduschi, Ana. 2019. "Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-discrimination Rights." *Big Data & Society*: 1–6.

Boston Consulting Group. 2015. "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries." https://www.bcg.com/publications/2015/engineered_products_project_business_

industry_4_future_productivity_growth_manufacturing_industries

Culik, Nicolai. 2018. "Brussels Calling: Big Data and Privacy." In *Big Data in Context: Legal Social and Technological Insights*, edited by Thomas Hoeren and Barbara Kolany-Raiser, 29–35. New York: Springer International Publishing.

De Mauro, Andrea, Marco Greco, and Michele Grimaldi. 2014. "What is Big Data? A Consensual Definition and a Review of Key Research Topics." Paper presented at the 4th International Conference on Integrated Information.

Elgendy, Nada, and Amed Elragal. 2014. "Big Data Analytics: A Literature Review Paper." *Lecture Notes in Computer Science*: 214–227. DOI:10.1007/978-3-319-08976-8_16

European Commission. 2017. Germany: Industrie 4.0. *Digital Transformation Monitor*. January 2017. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf

GSMA. 2018. "The Mobile Economy: Latin America and the Caribbean 2018." GSMA Intelligence. https://www.gsma.com/latinamerica/wp-content/uploads/2018/12/Mobile-Economy-2018-ENG.pdf

Hartmann, Philipp Max, Mohamed Zaki, Niels Feldmann, and Andy Neely. 2014. "Big Data for Big Business? A Taxonomy of Data-driven Business Models used by Start-up Firms" Cambridge Service Alliance, University of Cambridge. https://cambridgeservicealliance.eng.cam.ac.uk/resources/Downloads/Monthly%20Papers/2014_March_DataDrivenBusinessModels.pdf

Haupt, Michael. 2016. "Data is the New Oil": A Ludicrous Proposition. *Medium*. https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294

IMF. 2019. "Economic Outlook: The Americas." Washington, DC: International Monetary Fund.

Kleinberg, Jon, Jens Ludwig, Sendhil Mullainathan, and Cass R. Sunstein. 2018. "Discrimination in the Age of Algorithms." *Journal of Legal Analysis 10*: 113–174.

Lu, Yang. 2017. "Industry 4.0: A Survey on Technologies, Applications and Open Research Issues." *Journal of Industrial Information Integration 6*: 1–10.

Newman-Pont, Vivian, and María Paula Ángel Arango. 2019. *Accountability of Google and Other Businesses in Colombia: Data Protection in the Digital Age.* Bogotá, Colombia: Dejusticia. https://www.dejusticia.org/publication/rendicion-de-cuentas-de-google-y-otros-negocios-en-colombia-la-proteccion-de-datos-digitales-en-la-era-digital/

Organization of American States. 2015. Inter-American Juridical Committee. Privacy and Data Protection, March 26, 2015. http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI-doc_474-15_rev2.pdf

Pence, Harry. 2014. "What is Big Data and Why is it Important?" *Journal of Educational Technology Systems 43* no. 2: 159–171. DOI:10.2190/et.43.2.d

Todorov, Tzvetan. 2012. *The Inner Enemies of Democracy.* Cambridge, UK: Polity Press.

Vaidya, Saurabh, Prashant M. Ambad, and Santosh P. Bhosle. 2018. "Industry 4.0: A Glimpse." Procedia Manufacturing.

Zuiderveen Borgesius, Frederik. 2018. "Discrimination, Artificial Intelligence, and Algorithmic Decision-Making." Council of Europe. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

APPLICATION OF THE PERSONAL DATA PROTECTION LAW IN BRAZIL: A CASE STUDY OF SOME DATA-DRIVEN BUSINESSES

Kimberly Anastácio
Bruna Martins dos Santos
Joana Varon

This research was conducted by Coding Rights in partnership with Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia). Dejusticia coordinated a comparative research between Colombia, Chile, Mexico, and Brazil on the implementation of their personal data protection laws. Coding Rights analyzed the privacy policies and terms of service of online service applications offering services in Brazil to find out how they conform to the provisions of the Brazilian data protection law. Following the comparative analysis methodology defined for the study, four companies with data-driven business models (CDDBM) were selected. Hence, Amazon Prime Video was selected for the large Internet companies group; iFood was selected for the intermediate companies group; Social Miner was selected for the start-ups group; and Magazine Luiza was selected for the established companies group.

This article is divided into four sections. Section 1 describes the selection criteria for the companies analyzed and identifies four main aspects of their terms of service and privacy policies: 1) source of the data collected, 2) data processing, 3) purpose of processing, and 4) the relationship of the companies and the data collected with GAFAM companies. Section 2 analyzes how the practices of these companies conform to the Brazilian data protection legal regime. The practices of the companies selected are observed to outline the points that may be compared with the provisions of

the Personal Data Protection Law (LGPD) and other regulations regarding the protection of privacy and personal data, like the Consumer Defense Code, the Civil Rights Framework for the Internet, and the Constitution of Brazil. Section 3 evaluates whether the work of the National Data Protection Authority (ANDP), the entity in charge of monitoring the application of the Brazilian law, adequately addresses the practices of the companies mentioned above, mainly regarding the former's regulation, supervision, control, and sanctioning capacity. Finally, conclusions and recommendations are presented so that the operations of the CDDBMs are increasingly in line with the country's data protection principles and regulations, especially considering the need for companies to conform to the recently enacted law (LGPD), to become effective in 2020.

1. Selection of CDDBMs

1.1. GAFAM Company: Amazon Prime Video

This study analyzes both Amazon Prime Video's video-on-demand service and the specificities of its offer linked to Vivo, Brazilian telephone concessionaire and subsidiary of Telefónica. Amazon Prime launched in Brazil in September 2019, when this study was already underway. Before, since 2018, the telephone operator Vivo, began offering the video streaming service Amazon Prime Video to its customers, in partnership with Amazon. Therefore, in this study, we analyze the documents and policies in force before September 2019, when the service was offered jointly with Vivo. In this case, the company offers a 90-day-free trial; then, charges 7.90 reals during the first 6 months and, from the next month, 14.90 reals per month.[12] However, to subscribe, one must be a mobile or broadband customer of Vivo. Amazon also offers the plan directly in Brazil, but only offers a 7-day free trial; then the service also costs 7.90 reals per month for the first six months, and then increases to 14.90 reals per month.[13]

Besides the fact that this partnership with Vivo is considered interesting in terms of data protection, it is also important to analyze Amazon Prime Video in terms of Amazon's dispute with Google regarding the service. After several months of retaliation, both giants reached an

12. Current costs as of the date of access available on Vivo's website: https://www.vivoparasuacasa.com.br/amazonprimevideo/?gclid=EAIaIQobChMIIba8weX_4wIVIIaRCh3epwrjEAAYASAAEgKRIvD_BwE

13. Costs available as of the date of access on Amazon Prime Video's website: https://www.primevideo.com/

agreement, and the service became available for Chromecast in June 2019 (Gartenberg 2019).

1.2. Intermediate Company: iFood

iFood is a closed capital company founded in 2011 and currently operates in over 200 cities[14] in Brazil and in Mexico, Colombia, and Argentina. iFood is a food delivery platform. The service, offered on a web version and in applications for iOS, Android, and Windows Phone, serves almost 600,000 orders a day in Brazil to its 12 million active users (Daroit 2019). The company also has a product called iFoodLabs, an innovation laboratory focused on applying a business vision to ideas that combine food and technology. Using market data, experiences, clients' use cases, and interviews with stakeholders and specialists, the laboratory designs methodologies to create solutions for the delivery segment of the food supply chain. The laboratory created products such as the SpoonRocket[15] and iFoodNext, a division focused on developing software and services focused on the demands of restaurant owners. The company also has a platform called iFood Shop (Belloni 2018), which connects restaurants with packaging and supplies providers.

The start-up has received contributions by companies such as Móvile, which invested 5.5 million reals in 2013 (Zuini 2013) and 125 million reals (together with the British company Just Eat) in 2015. In November 2018, Móvile announced that iFood would receive an investment of 500 million dollars (Brigatto 2018), equal to 1.9 trillion reals—the largest investment by a private technology company in Brazil. The idea of the investment was to extend iFood's operations in the country and double the number of restaurants (currently about 66,000) and the cities served (500 municipalities; Freitas 2019b). iFood is the 23rd most downloaded app on the Play Store. The application has over 10 million downloads and is the most downloaded app in the "Food & Drink" category on the Play Store.

1.3. Start-up: Social Miner

The company is on several "start-ups to watch" lists in the country for drawing the attention of start-ups acceleration programs led by companies

14. iFood "Cidades Atendidas" (no date). Retrieved August 15, 2019. from https://www.iFood.com.br/cidades-atendidas.

15. Available at the application's website: https://www.spoonrocket.com.br/

like Oracle[16] and Google (Freitas 2019a). The company does not have an app; however, it developed a proprietary online targeted advertisement platform. Created in 2014, it declares that its objective is "to bring brands and people closer to technology and improve their respective online performance by combining Artificial Intelligence and Big Data."[17] The company identifies consumer habits, consumer profiles, and online engagement methodologies with brands through a database. This database is capable of identifying the "phase of the consumer decision journey and also the purchase intention"[18] to help companies direct targeted advertisements/engage visitors who would not buy their products.

Social Miner is a company whose products have no interaction with the end users, as it offers digital engagement and marketing strategies to companies or its clients. According to the company's website, Social Miner offers a platform that allows its clients[19]—which include Avon, Asus, Sephora Brasil, Natura, Extra, and Wine.com.br—a better understanding of the ideal contexts and languages to encourage dubious consumers, segment their data, and create personalized campaigns.

1.4. Established Company: Magazine Luiza

Magazine Luiza is a retail company whose digital strategy drew the attention for products such as a bot—Lu—who has her own YouTube channel, for programs that encourage their stores to produce content for Facebook, and because its app has over 10 million downloads in Brazil's Play Store[20] and holds the second place in the most downloaded shopping apps in Brazil's App Store.

Established in 1957 in Franca, São Paulo, the brand owns over 900 physical stores and 12 distribution stores in 17 Brazilian states.[21] It offers products in the furniture, home appliances, electronics, presents, toys,

---

16. "Social Miner no Oracle Start-up Cloud Accelerator," 2018. Social Miner: http://blog.socialminer.com/people-marketing/social-miner-no-oracle-startup-cloud-accelerator/

17. Social Miner, "Sobre Nós" (no date). Retrieved July 25, 2019, from https://socialminer.com/sobre-nos.html

18. "Social Miner Cases de Sucesso" (no date): https://socialminer.com/

19. Social Miner, "Sobre Nós" (no date).

20. Google Play Store, "App do Magazine Luiza" (no date). Retrieved August 15, 2019, from https://play.google.com/store/apps/details?id=com.luizalabs.mlapp&hl=pt_BR

21. *Magazine Luiza*, "About Us," 2019: https://ri.magazineluiza.com.br/ShowCanal/Quem-Somos?=urUqu4hANldyCLgMRgOsTw==

hobby and entertainment, informatics, and telephones sectors in physical stores, its website, and its application. Magazine Luiza introduced the concept of virtual stores in 1991, when its stores did not have physical products (Gazzoni & Cruz 2011). At this time, they conducted sales through electronic terminals and delivered the product up to 48 hours after purchase. The brand is still using the virtual store model, allowing the existence of stores with no physical supplies or displays. In 2013, the company introduced its virtual sales assistant—Lu—to assist users on the use of connected products, improve browsing on the website (Calado 2018), and contribute to its customers' digital inclusion (Fraga 2018). This digital avatar helped increase online sales by 56% during the first half of 2017 (Bloomberg 2017) and even has a YouTube channel[22] with now 2.3 million subscribers.

The company has typical strategies to develop its digital platform—in addition to the applications mentioned above: its website, virtual stores, YouTube channel, and avatar—Magazine Luiza was also a pioneer in the operation of retail sales through omni-channel (Ricciardi 2016) in Brazil. Omni-channel's operation allows various sales channels to use the same infrastructure (distribution centres, accounting, marketing). Some of the company's digital strategies are noteworthy. These include the Maga Local program, the Marketplace, and even its marketing actions on Tinder, which gave special discounts to users who matched with Lu's profile (Bloomberg 2017). The company's Maga Local encourages the stores to have their own Facebook fan pages and autonomy to produce their content. The Marketplace, launched in 2016, currently offers products from over 500 companies in Magazine Luiza's application and website, and represents one fourth of its digital sales (Magazine Luiza 2019).

In an article published in October 2017, Magazine Luiza's CEO, Federico Trajano, mentioned that the company intended to counter Amazon's expansion in Brazil with possible reinforcements in its physical stores and by integrating the online and physical stores. At the time, Internet sales amounted to 30% of Magazine Luiza's income, approximately 4 trillion reals, and the application had 7 million monthly visits (Manzoni 2017).

---

22. Canal da Lu – Magalu, YouTube. Retrieved July 15, 2019, from https://www.youtube.com/user/magazineluizacom

2. Characterization of CDDBMs' Operations

2.1. Data Sources

Amazon Prime Video's job listings describe how the company intends to "mould the future of video entertainment." For example, by hiring people for positions like Business Intelligence Engineers it seeks to "discover how users watch videos on amazon" and "work with one of the world's largest user databases" (LinkedIn n.d.). Another position offered is the head of the data engineers and scientists team, responsible for "defining and delivering behavioural metrics and client marketing" (Higa 2019). The collection and processing of its users' data is undoubtedly at the core of the business.

In Brazil, these services are also offered in partnership with Vivo, the mobile operator, which, like many others, was investigated (Luna 2018) for suspected personal data use.

According to Vivo's website, anyone with a subscription to their mobile plans only needs to send an SMS with the word "Amazon" to subscribe to Amazon Prime Video. The platform is even making partnerships to produce content in Brazil (Meio and Mensagem 2018). Thus, the user of this service will be subject to Vivo[23] and Amazon's terms of service[24] and, in the event of a conflict between them, Vivo declares that its terms shall prevail.

The data sources come from both the provisions of Vivo's Privacy Center[25] and Amazon's Terms of Service[26] and Privacy Notice.[27]

Amazon Prime Video's terms of service, which are part of Vivo's service subscription agreement, or by searching on Amazon to directly hire the service with the foreign company, mention that Amazon's Video Marketplace has different vendors and, therefore, different applicable terms

---

23. "Vivo para su casa" (no date). Retrieved August 15, 2019, from https://www.vivoparasuacasa.com.br/amazonprimevideo/?gclid=EAIaIQobChMIIba8weX_4wIVII Arch3epwrjeaayasaaegkrivd_Bw (el servicio ya no existe).

24. "Termos de Uso do Amazon Prime Video" (no date). Retrieved July 15, 2019, from https://www.primevideo.com/region/na/help?nodeId=202095490

25. "Centro de privacidade" (no date). Retrieved August 15, 2019, from https://www.vivo.com.br/portalweb/appmanager/env/web?_nfls=false&_nfpb=true&_pageLabel=vivoVivoInstPrivacidadePage&WT.ac=portal.amarca.privacidade&# (el servicio ya no existe).

26. "Termos de Uso do Amazon Prime Video" (no date).

27. "Amazon Privacy Notice" (no date). Retrieved July 15, 2019, from https://www.amazon.com/gp/help/customer/display.html?nodeId=468496

and policies that vary between regions. Mexico is the only Latin American country explicitly mentioned. Brazilian consumers are grouped under the category "United States and all other countries and territories" whose vendor is Amazon's headquarters in Seattle. The applicable terms and legal notices are the following; some of which are only available in English:

- Amazon Prime Video Terms of Service (available in PT)
- Amazon Prime Video Usage Rules (available in PT)
- Condition of Use (only available in ENG)
- Privacy Notice (only available in ENG)
- Interest-Based Ads Policy (only available in ENG)
- Twitch Terms of Service (only available in ENG)

The "Software" section of Amazon Prime Video's terms of service mentions that "the Service may provide Amazon with information relating to your use and the performance of the Service, as well as information regarding the devices on which you download and use the Service and Software."[28] There, it includes information on how the digital content of the platform is consumed.

Amazon Prime Video's terms of service and usage rules do not contain anything else on data protection, but state that said information is subject to Amazon's Privacy Notice, available only in English, even for those hiring the service in Brazil.

These documents emphasize that Amazon recognizes that it may collect the following types of data and information: 1) information we provide; 2) "automated information," mentioning the use of cookies; 3) information on our devices, including the confirmation of the receipt/reading of communication emails it sends to its customers, and 4) "information from other sources," including the shipping address, purchase data, site visits, search results or searches made through Alexa, and even information on our credit history provided by credit bureaus.

Vivo's Privacy Center describes the collection of information on 1) registration data such as the name, address, CPF, and others, as mentioned in the contract; 2) volume of data transferred on the Internet; 3) history of use of the products and services hired which, according to the company, does not involve registries of applications other than Vivo nor

28. "Termos de Uso do Amazon Prime Video": https://www.primevideo.com/help/ref=atv_nb_lcl_pt_BR?_encoding=UTF8&nodeId=202095490

of social media activity; 4) incoming calls and SMS history; 5) accounting and tax information and customer support data.

For its part, according to iFood's privacy policy, the company collects and processes data from three primary sources. First, the data provided by the user/customer. Upon signing up, the user agrees to provide information such as their name, address, CPF, email address, telephone number, and date of birth. When users continuously use the application or website, the company collects data on the platform's user behaviour, tracing the purchase and activity history within the application. Furthermore, it collects data on the payment method, including the client's credit card numbers. A critical part of the application's operations is the collection of location data, which may be provided by the user or collected by the GPS and the mobile networks of the registered cellphone. According to the privacy policy, such information "shall be considered as registration data [...] for the effects of Law No. 12.965 of 2014 (Civil Rights Framework for the Internet), or any law that replaces it." (Government of Brazil, 2014).[29]

The second source is data shared by strategic partners. In this case, a client may directly log in with their Facebook account, allowing iFood to collect the data from this site directly related to the client's identity, such as their name, gender, and age. The third source of data is web tracking. According to its privacy policy, iFood may automatically collect information from the devices used to use the application, including "IP addresses, type of browser and language, Internet service provider (ISP), search and exit pages, operating system, date and time information, click stream data, device manufacturer, operator, model, Wi-Fi networks and telephone number."

iFood's privacy policy also mentions that the information about users' activities on the web or application will be considered as aggregate data and non-personal information. The policy also states that "the age of the individual, its preferences, the language, the CEP, and the area code" are considered non-personal information, provided they are not combined with the personal data of the particular individual.

Regarding Social Miner, in an article published on the website "Proyecto Draft" (Souza 2016), the company was quoted as a promising

29. Government of Brazil, Lei 12.965, "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet)." April 23, 2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

initiative that "uses artificial intelligence, social profiling, and communications to automatize digital marketing campaigns with a high level of customization." Social Miner claims that it introduced the human factor to previously developed digital marketing technologies with the concept that these define "people marketing"—or the provision of bespoke routing. According to the same article, the commitment of Social Miners is as follows:

Imagine that you are browsing an e-commerce site that hires Social Miner, and you decide to leave the site. Upon noticing the mouse cursor's movement toward the edge of the screen, the algorithm perceives that you will not make a purchase at that time and offers you a benefit, which might be a coupon or even access to exclusive suggestions, to stay in touch with the brand. It may also be a pop-up (which does not prevent you from closing the site).

When the user decides to log in through Facebook, the platform obtains data enabling them to call you by your name and direct content, for example, according to your city, sex, and age range. After signing up, Social Miner's algorithms begin to track your browsing profile in the website to understand the user's behaviour, the products seen, whether or not a purchase was made, etc.

After collecting this information, it is time to talk to the user, at just the right time (Souza 2016).

Concerning the above, it is clear that the content routing offered by Social Miner is fed by the users' browsing and login data from platforms such as Facebook. With the data collected and services offered the start-up published the report entitled "O comportamento do consumidor Online em 2018."[30] This report contains an analysis of the consumption profile of 35 million people registered in their database and e-commerce websites performance statistics.

People marketing—a concept developed by Social Miner—has drawn the attention of start-up acceleration programs led by companies like Oracle (2018) and Google. The 5-year-old company has also received investments from funds such as Canary, Wayra (Grupo Telefónica), and Indicador Capital.

30. See https://conteudo.socialminer.com/relatorio-comportamento-do-consumidor?utm_source=ECBR&utm_medium=artigo&utm_campaign=relatorio-comportamento-do-consumidor-2018

The company claims that it acts according to the European regulations and ensures the safety of its user's data and privacy. Therefore, this tool lists eight rights of the users affected by the company. This list includes, among others, the right to be informed of any data collected and demand adjustments in the collection, the right to forbid the collection of new data, and the right to "contest decisions made by automated means, or profiling, if such decisions would have the power to produce legal, or other equally significant effects."[31]

Regarding the collection of data for the proactive contract of the sales team, Social Miner collects data such as the name, email address, telephone number, company's website, business sector or category, and company's website traffic "every time a visitor downloads any educational material, registers on our website or participates in any webinar or event organized by Social Miner."[32]

Furthermore, every time a user browses the company's website, the visit is transformed into data processed by Google Analytics. If a connection is made through Facebook, i.e., when the user signs up through Facebook, the profile's public information is also collected. "If a user opts in by clicking on the notifications of the website, the name, email address, and cookies information are collected."[33]

Regarding the operation of the platform and the collection of data of users browsing the websites of Social Miner's clients, the data collected are the same as mentioned above, when the users opt-in. The tool is heavily supported by the collection and analysis of cookies. Therefore, the company has a separate document: their "cookie policy."[34]

This policy states that Social Miner uses "persistent" cookies, that is, "all those which, regardless of browsing, are always registered on Social Miner server," and "session cookies," that is, the "browsing behaviours within a single user's browsing window."[35]

For the company, session cookies are divided in:

1. Analysis cookies, which allow recognizing and counting visits.

---

31. Social Miner, "Política de Privacidade" (no date): https://socialminer.com/privacidade.html

32. Ibid.

33. Ibid.

34. Social Miner, "Política de Cookie" (no date): https://socialminer.com/cookies.html

35. Ibid.

2. Recognition cookies aimed at recognizing the feedback of the website or technology users.
3. Tracking cookies, which record visits to the website or technology, the pages visited, and additional browsing information. Furthermore, the privacy policy states that:

> When someone becomes Social Miner's client, we use connection plugins, especially Facebook Login, to create a user database for the client's brand. The connection warnings and windows may appear at the start or the end of each user's browsing session when he or she shows the intention of leaving the website so as not to hinder browsing or interfering with the eventual purchase procedures.[36]

Regarding Magazine Luiza, the company's privacy policy starts by clarifying some initial definitions for the effects of the document:

> Cookies: files sent by the website's server to the user's computer to identify the device and obtain access data such as pages browsed or links clicked, thus allowing customizing the website's use according to the user's profile.
>
> IP: abbreviation for Internet Protocol. It is a set of numbers identifying the user's computer on the Internet.
>
> Logs: records of the user's activities on the website.
>
> Session ID: identification of a User's session in the sign-up process or when the website is used in any way.
>
> User: anyone who uses the website.[37]

Magazine Luiza's e-commerce and application have the same privacy policy issued on July 23, 2015. The document provides that the collection of data will take place from the moment the user: "(a) starts using the website; (b) interacts with the various tools available on the website, voluntarily providing information; or (c) contacts us through the communication channels available on the website."[38] To sign up on the website and the application, the user must be at least 18 years old and must provide

---

36. Social Miner, "Política de Privacidade" (no date).

37. "Política de Privacidade," 2015, *Magazine Luiza*: https://www.magazineluiza.com.br/politica/

38. Ibid.

the following data: full name, username, CPF, RG, full address, telephone number, date of birth, and email address.

However, a hot page of the application on Google Play clarifies that it may collect data such as the user's approximate location (via the mobile network) and exact location (via access to the GPS). Furthermore, the application asks for authorization to make calls directly, access the data on the user's cellphone SD card and points of use such as the data to install the API, direct access to the Internet, read Google's configuration services, receive data from the Internet, and access the network and Wi-Fi connections.

In addition to the data mentioned above, the company's privacy policy states that it may collect data on the user's activity on the website by using logs. The logs include the user's IP address, actions on the website, pages visited, date and time of access to the website's functionalities and type, and user's ID session.

2.2. Processing and Purpose

Amazon's Privacy Notice states that "we collect your personal information in order to provide and continually improve our products," and the document on "Interest-Based Ads" covers the practice of targeted advertisement. According to its Privacy Notice, the information is shared with 1) "affiliated businesses we do not control," 2) "third-party service providers" performing functions on Amazon's behalf (to send offers to specific groups; in this case, opting out is possible), 3) in the event Amazon buys or sales business units, and 4) in the case of protection of Amazon.com and others for fraud suspicion or other purposes. Finally, after listing these processing cases and the other purposes for sharing information, the document states that in the cases that data may be shared with third parties, its consumers are notified to express their consent or opt-out from sharing their data.

Vivo's Personal Data Processing terms are available on its Privacy Center,[39] unlike what the Privacy Central states, the terms do not classify the data source nor mention the types of processing, but provide that the contracted party, in this case, Telefónica, has the obligation of processing personal data as necessary to provide the service, forbidding

39. Telefônica, Termo de Tratamento de Dados Pessoais, July 1, 2019: https://www.vivo.com.br/portalweb/ShowPropertyServlet?nodeId=/ucmrepository/contrib_269712 (el servicio ya no existe).

the processing for other purposes without express authorization. Then, it mentions other obligations, including transparency, to process its customers' data.

Regarding the Privacy Central, it provides examples of the reasons to collect data from its clients:

> (a) credit use and recharge transactions; (b) improve the network performance and correct faults; (c) customize plan development processes, (d) assess demand by region; (e) inform Vivo's strategic decision-making by redistributing the signal or reorganizing the service portfolio; (f) direct marketing.

Therefore, note that the information on the same subject—data processing—is scattered and presented differently in different documents or information sources. Nor is it clear on items (c) and (f) if the personal data is used for profiling.

In its privacy policy,[40] iFood states that the data collected are used to improve its services, develop new services, and to promote auditing and statistical analysis on the use of services, including consumption trends and "services and communication with its clients," with no further details on what these services include. Still, the company makes it clear that it will use the shopping feedback data, that is, the user's receipt confirmation of its purchase on the application, to "publish and use said comments and feedback on the website or the application and any marketing or advertisement material, and to analyze, process or handle that feedback in an isolated or aggregate manner." To this end, the application identifies the client and its feedback "through its username, iFood profile picture (if any), and city of residence." Furthermore, it provides that the data is also used to "analyze and solve technical problems, and to identify and prevent fraud in the use of [...] the Service" and to send notifications and essential communications, such as changes in the policies, changes in the terms, and communications that may not be disabled by the customer because they are considered inherent to the service. A specific section of the privacy policy shows the possibility of using the data for digital (social media sites routing and push notifications) and non-digital (radio, leaflets, outdoors) marketing purposes.

40. iFood, "Privacy Policy," 2018. https://www.iFood.com.br/privacidade

Another section explains the collection of data by cookies and similar technologies. According to the section, "iFood uses technologies like cookies, *pixel tags*, local storage or other identifiers in mobile devices or otherwise, or similar technologies ('cookies and other technologies') for several purposes," for instance, to "authenticate your account, promote and improve iFood services, customize your experience and evaluate the efficiency of our communication and advertisement."[41] For iFood, this information is not considered personal, provided it is not combined with personal data.

In fact, the company's policy presents the clients with examples of the use of such data:

Knowing your first name allows us to welcome you the next time you sign in into iFood. Knowing your country and language allows us to provide a customized and more convenient purchase experience. Knowing that you bought a product or used a specific service allows us to make our advertisement and email communications more relevant for your interests.[42]

Regarding third parties, iFood states that it might share the data with its partners to develop more assertive marketing campaigns, and that it will "share the data only with partners whose privacy policy offers protection levels similar to those offered" by their policy. Furthermore, third parties conducting marketing activities in iFood's application or website, that is, which promote the advertisement of third-party products in such spaces, "may use cookies or other proprietary technology in iFood's services, such as Facebook, Google Analytics and Double Click" to test the performance of marketing campaigns.[43]

The privacy policy states that the members of iFood group may also access some of its clients' data, as well as to the payment processing companies, the related companies delivering the orders, social media services (for example, when a client shares a recent purchase directly on Facebook) and, in the case of data such as the name and profile photo, with other users of the application.

The company also states that data is stored in "reliable cloud services of partners located in Brazil or elsewhere offering reliable cloud

41. Ibid.
42. Ibid.
43. Ibid.

storageservices commonly used by technology companies" and retained for the time prescribed by the applicable laws.[44]

The company even intends to comply with the laws on data transfer for the legal authorities. However, it goes further stating that "iFood reserves the right to share information of its users with third parties when there is sufficient reason to believe that a user's activity is suspicious, illegal or detrimental for iFood or any third party."[45]

Regarding security, iFood claims that it follows "privacy by design." The company does not specify what this means, but in the same section, states that "we only process your data with a high degree of security."

On their part, in the opening statement of Social Miner's privacy policy, the company recommends those who "do not agree with the contents of the policy not to download our materials nor use any of our services and, if you already downloaded them or used them and want to exercise your right to restriction, rectification, cancellation or opposition, contact us at privacy@socialminer.com."[46]

On the use of data, the company claims that the marketing team will use the data collected for a proactive contract with the sales team. Furthermore, the company claims that it may cross-reference the data collected via Facebook's login with the browsing data "to allow for greater customization of the messages our company sends" to clients.[47]

The data collected from users on the websites of Social Miner clients may even be used for "greater customization of the messages the company (the contracting party) sends, whether as automatic analysis of the purchase behaviour made by the artificial intelligence algorithms," developed by the company.[48] In other words, cross-referencing data, especially the browsing cookies, enable the customization of advertisements displayed to the users entering the websites that hire Social Miner's services.

Thus, the personal data collected from the users are automatically used and processed by the algorithms to understand behaviour patterns and create segmented audiences for the platform's campaigns. According to the privacy policy, the company uses "automation to process data to analyze the user or visitor's movements on the website, identifying the

44. Ibid.
45. Ibid.
46. Social Miner, "Política de Privacidade" (no date).
47. Ibid.
48. Social Miner, "Política de Privacidade" (no date).

contents and products of interest and, based on this, customize product suggestions according to individual preferences."[49]

According to the policy, the "general signup and click data will be used to optimize the campaigns created by our platform and will always be available (to the contracting parties), allowing their extraction at any time or their integration to the CRM software (of the contracts)";[50] CRM is the acronym for "Customer Relationship Management," a tool that facilitates the subscription and registration of each customer's information. According to the document, the contracting party's website users have the right to unsubscribe from the database. However, it is not clear how this request works and how the users learn about it.

Furthermore, the privacy policy states that the data collected by the company will also "be used for eventual service charges, internal communications, and send educational materials or conduct market research." Regarding this research, Social Miner states that "the data used for general studies on consumer behaviour will delete the user's personal information," and that, in this case, these data are no longer personal but a "set of anonymized data collected for study and research purposes."[51]

Regarding the protection of the data collected, the company claims that the access to personal data "is restricted to Social Miner's employees, more specifically to the sales, finance and marketing departments" and that no personal information may be publicly disclosed. Furthermore, the company states that "it agrees not to sell, lease or transfer your information to third parties" unless required by law.[52]

The contracting party accesses user data based on user behaviour and the customization of campaigns, without the former directly accessing the user's individualized behaviour on Social Miner's platform. Furthermore, the company claims that it is against "cookie pooling," the practice of sharing cookie databases among its clients, that is, among the contracting companies' websites.

Finally, it notes that the policy states that "if you are a user visiting the site of one of Social Miner's clients, we recommend contacting the client to exercise your rights to privacy."[53] It also states that it does not

---

49. Ibid.
50. Ibid.
51. Ibid.
52. Social Miner, "Política de Privacidade" (no date).
53. Ibid.

collect data from children under the age of 13. The company states that it keeps the data for as long as necessary to provide its services, as long as they have the consent for it or as determined by the law, deleting inactive data after five years.

Magazine Luiza's privacy policy clarifies that the data and the information collected will be aggregated into their website data bank, owned by the company. The relevant data will be stored in a secure environment to which only qualified and authorized persons will have access. However, the company is exempted from possible damages caused by faults, viruses, or intrusions into the website's data bank, except in cases of willful misconduct or negligence by the company.

The company also mentions that user data will not be shared, sold, or disclosed to third parties. Furthermore, it provides that the website's user and the data subject may add, exclude, or modify any information linked to its profile.

Regarding the processing of data, the privacy policy mentions that the personal data collected may be used for the following purposes:

1) Issue any communication resulting in an activity of the website or identify the relevant addressee; 2) Respond to eventual doubts or queries by the user; 3) Provide access to the website's restricted area or exclusive functionalities; 4) Comply with a legal or judicial order; 5) Regularly constitute, defend or exercise rights in judicial or administrative proceedings; 6) Prepare general statistics to identify user profiles and develop Magazine Luiza's campaigns; 7) Ensure user's security; 8) Maintain the user subscription up to date to make authorized contact via telephone, email, SMS, physical mail, or other means of communication; 8) Inform about news, promotions, and events of Magazine Luiza and its commercial partners.[54]

The company also reserves the right to send daily emails with offers to subscribed clients. The user may unsubscribe from receiving these messages through a link included in all the promotional emails.

Finally, regarding cookies, MagaLu states that it may use them and that the user may disable them on their browser of choice. Regarding activity tracking data, the company reserves their use to investigate cases of fraud or undue alteration to its systems or subscriptions.

54. Social Miner, "Política de Privacidade" (no date).

2.3. Relationship with GAFAM Companies

Amazon Prime Video maintains a direct relationship with the Brazilian company Vivo, affecting the understanding of the extent of the relationship between these two companies and data. The multiple documents on the matter in both platforms make an informed comprehension unfeasible for the everyday consumer or even consumers familiar with the debate on data protection.

Considering the connection between iFood and GAFAM, there are three types of relationships. First, the company allows users to access their accounts through their Facebook profiles. The other option is by creating a new account with the personal email, but this option is less prominent in the application. Second, the privacy policy declares the possibility of social media buttons, where the user may directly share the details of their orders on Facebook. Third, iFood uses Google Analytics, collecting information on the behaviour of the website's users to map trends.

This way, iFood makes information available to GAFAM and collects data from them. For example, regarding Facebook, the privacy policy states that:

> By using Facebook to sign up for our service, you allow iFood to access your Facebook account's personal information, including your name, gender, age, and telephone number (if registered on Facebook). In this case, the information we may obtain depends on your privacy settings on the social media site.[55]

Upon analyzing the relationship between the application and iFood, in 2018 a rumour spread on the Internet that affected some Facebook profiles. Some users changed their surname to "iFood" on Facebook to receive a discount coupon on the application. However, the coupon was a lie, and the users who made the change were forced to maintain said name for at least 60 days due to the platform's policies (Letieri 2019). iFood also had the initiative to create a bot that interacted with users through Facebook Messenger, so that the users could make orders directly on the social networking site. This feature is no longer operational (Letieri 2019). Furthermore, Google can make purchases through mobile applications faster via "Pay with Google;" this option works to make purchases on iFood and Magazine Luiza (Gazeta Do Povo 2017).

---

55. Social Miner, "Política de Privacidade" (no date).

Regarding the relationship between Social Miner and the GAFAM companies, the company reserves the right to cross-reference browsing data and the Facebook login to perfect the products offered. The content routing platform offered by Social Miner feeds with the user's browsing data and the login data of platforms like Facebook.

The company's privacy policy mentions that the visitors' browsing data will be transformed into data by Google Analytics and that, if the visitor signs in through Facebook, it will use necessary public information such as name, age, sex, and browsing data to allow for greater customization of the messages sent by the company.

The document mentions the use of connection plugins, especially Facebook login, to create a database of users/customers for the contracting brand. Furthermore, the company offers the capability of showing notifications and social network connection screens at the beginning of browsing or whenever the consumer wishes to exit the website of a specific brand. In other words, the eventual collection of personal data by Social Miner to create databases might not be duly informed to the consumer.

Regarding MagaLu, the clear connection between the website and the application, and GAFAM, is through the authentication with the Facebook profile or Google account. However, the application clarifies that no content will be published on behalf of the account holders. Furthermore, both platforms allow sharing offers via Facebook, Twitter, Google Plus, WhatsApp, and email. The privacy policy does not mention anything on the shared use of data with the platforms or the use of Google Analytics to analyze the users' purchasing behaviour.

However, the digital strategy of the company is mostly involved with Facebook. In 2012, MagaLu presented the idea of enabling the stores on Facebook's platform and building an e-commerce network where users could establish their stores affiliated to Magazine Luiza (Jesús 2012).

Another internal program of the company, called Magazine Você, intended to remunerate users with small commissions if they recommended specific products on social media. According to the website Tecnoblog (Veloso 2012), the program worked as follows:

By having a Facebook account, the social media site users could use the Magazine Você application to recommend products offered by Magazine Luiza to their friends. The operating logic is similar to that of any loyalty program: a commission per item sold, equal to a percentage of the sale value.

By having a Facebook account, the users of the social media site can use the application.

The company's website has no information on Magazine Você, and the program's Facebook page is no longer available.

3. Evaluation of the Personal Data Protection Legal Regime to Address the Dynamics of the Companies Analyzed

3.1. Brazil's Data Protection Legal Regime

Brazil has had a General Personal Data Protection Law (Law 13.709/2018) since 2018.[56] This law has been subject to political arrangements and intense discussions among the country's stakeholders. However, even before it was passed, Brazil had preceding laws that safeguarded the right to privacy to some extent. The Federal Constitution, the Consumer Defense Code (Law 8.078/90),[57] the Habeas Data Law (Law 9507/97), and the Civil Rights Framework for the Internet (Law 12.965)[58] and its regulatory Decree (Decree 8.771/16) defined the principles and guidelines for privacy protection (Privacy International 2019). Furthermore, several specific regulations (Monteiro 2017) also deal, albeit tangentially, with personal data protection, mainly in the financial and healthcare systems. However, the Civil Rights Framework for the Internet, a law enacted in 2014, was the first law to deal specifically with data protection on the Internet until the LGPD was passed.

Following a series of consultations with various industries, the Civil Rights Framework for the Internet became an internationally known and

---

56. Government of Brazil, 2018, "Lei Geral de Proteção de Dados Pessoais" [LGPD; Personal Data Protection Law]. Law 13.709, August 14, 2018. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. See also Medida Provisória n. 869. December 27, 2018. Altera a Lei nº 13.709, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. August 14, 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869impressao.htm

57. Government of Brazil, 1990, Lei nº 8.078, "Dispõe sobre a proteção do consumidor e dá outras providências." September 11, 1990. http://www.planalto.gov.br/ccivil_03/leis/l8078.htm

58. Government of Brazil, Lei 12.965, "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet)." April 23, 2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

renowned law. It served, among other things, as a letter of rights and duties on the Internet in Brazil. It was also the primary guideline to develop the LGPD regarding the protection of personal data, the rationale of the right to privacy, and the concept of consent to Internet agreements.

For example, said law presented significant initial provisions on protection and on sharing users' data. Articles 10 and 11 emphasize the importance of care in collecting, processing, and transmitting user data on the Internet. For instance, these articles establish that Internet providers may only provide access and connection logs to Internet applications by means of a court order. Specifically, Article 11 states that:

> In any operation to collect, store, protect and process logs, personal data or communications by connection providers and Internet applications in which at least one of this acts is carried out within the national territory, they shall adhere to the Brazilian laws and the rights to privacy, the protection of personal data, and the secrecy of the logs and private communications.

Even more so, the law defends the "inviolability of intimacy and privacy, its protection and compensation for material or moral damages resulting from their breach" while using the Internet (Article 7). Specifically, the Civil Rights Framework for the Internet also set the grounds for what, with some exceptions, the LGPD would consolidate as one of the measures required to collect data: user consent. Article 16 of the Framework states that:

> In the provision of Internet applications, whether free or at cost, it is prohibited to retain: I—the records of access to other Internet applications without users' prior and express consent [...] II—personal data that exceeds the purpose for which consent was given by the owner of the data.

By only dealing with the Internet, the Civil Rights Framework did not solve the gray areas regarding data protection in Brazil. However, it did point out some principles and responsibilities. Incidentally, even before adopting the Civil Rights Framework, other laws had already been used to assert data protection issues. They were already being constructed to give continuity to what would later become the LGPD. For example, Article 43 of the Code of Consumer Protection (CDC), issued in 1990, states that:

> Consumers [...] shall have access to the information in registries, records, and files on their personal and consumption data and their respective sources. Consumer registers and data shall be objective, transparent, truthful, and in an easily comprehensible language, being hereby prohibited from containing backup information referring to the last five years.

It also states that the consumer may demand the correction of inaccurate data. Despite being drafted at a time when commercial Internet did not yet pose the privacy challenges it does nowadays, the CDC already provided an input that could be used to protect the user, albeit tangentially.

Discussions on the LGPD began in 2010, when the Ministry of Justice promoted a public consultation on the matter, and ended when the Federal Government submitted a bill to the National Congress. This bill was paired with other provisions already being debated and was discussed in Special Commissions. After two years of debates with numerous public hearings and consultations, its contents were passed and enacted in 2018. The law solved the eventual conflicts between the current norms and brought Brazil closer to the international trend of establishing a general data protection law.

By late 2019, the Brazilian government issued two decrees—10.046 and 10.047—which provide the governance and sharing of personal data within the competence of the federal public administration and create the Citizen Base Registry and the Central Data Governance Committee (Government of Brazil, 2019a, 2019b).[59] Although the decrees' initial proposal was to propose a greater harmony between the government's personal data processing and collection activities, the text is confusing and contains new definitions for some of the concepts addressed in the

59. Government of Brazil, 2019, Decreto n. 10.046, "Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados." October 9, 2019. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm; Government of Brazil, 2019, Decreto n. 10.047, "Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais." October 9, 2019. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10047.htm

LGPD. The National Congress of Brazil is now debating the derogation of both decrees.

3.2. Main Aspects of the Data Protection Law Regarding the Practices of the Four CCDBMs Analyzed

Considering the practices presented in the privacy policies and the terms of service of the four CDDBMs selected, below we analyze their compliance with the law to become effective in August 2020, and whether the law is sufficient to face the challenges the privacy policies pose.

3.2.1. Purpose, Consent, and Sharing of Information with Third Parties

The LGPD defined personal data as information regarding an identified or identifiable natural person. Article 6 of the law lists a series of principles that should guide the processing of personal data. According to this article, these are purpose, suitability, necessity, free access, quality of data, transparency, security, prevention, non-discrimination, and responsibility and accountability.

In addition to these principles, the law provides that the private sector requires consent to process personal data, except when complying with a legal obligation and other specific exceptions, such as the cases of a legitimate interest of the controller. In that specific case, the law provides that "when the processing is based on the controller's legitimate interest, only the personal data which is strictly necessary for the intended purpose may be processed" (Article 10, paragraph 1). Article 7, paragraph 5 of the law also provides that the controller who has obtained the consent and needs to communicate or share personal data with other controllers shall obtain specific consent from the data subject for this purpose (also considering the consent waiver hypothesis).

The law also provides that the consent must appear highlighted to stand out from the other contractual clauses, shall refer to particular purposes, and may be revoked at any time. The subject also has the right to facilitated access to information concerning the processing of his/her data, regarding:

1. The specific purpose of the processing.
2. The type and duration of the processing, observing commercial and industrial secrecy.
3. Identification of the controller.
4. The controller's contact information.

5. Information regarding the shared use of data by the controller and the purpose.
6. Responsibilities of the agents that will carry out the processing.
7. The data subject's rights, with explicit mention of the rights provided in Article 18 of this Law.

In regard to the analysis of the companies' practices in the light of the LGPD's provisions on consent, data sharing with third parties, and the principles, some aspects are worthy of attention.

For instance, in the case of Social Miner there is no clarity on how the user provides consent for his/her data to be included in the company's database. The consent to collect browsing data, covered by the collection of cookies, is given by the users accepting the notifications that appear in the upper or lower corners of the screen of Social Miner's clients websites. However, it is unknown whether there is an informed text pattern to users on each client's websites or whether the cookies tracking notifications are specific or sufficient for the user to understand that the collection will be used not only to improve browsing but also for explicit digital marketing purposes.

Furthermore, the privacy policy states that the data collection warnings "may appear at the start or end of each user's browsing session, when he or she shows the intention of leaving the website so as not to hinder browsing or interfere with any purchase procedures."[60] Every time, and at the start of the browsing session, users should be informed about the possibility that their data will be collected to obtain a greater and faster understanding of it.

Furthermore, the company has extensive provisions on data shared with third parties. According to the privacy policy, "Besides Social Miner, no other company or client will have access to the personal data of its leads. We are against cookie pooling and will never share our database with our clients."[61] This provision is appropriate, as it takes the user's privacy into account, but could have been included in the privacy policy due to the pressure of the cookies-based marketing market, which broadly rejects cookie pooling.

The other companies analyzed have strong positions regarding consent and data shared with third parties. In the case of Amazon Prime Video,

60. "Política de Privacidade" (no date).

61. Ibid.

this is even more complex, starting with the difficulty of finding the privacy policy that governs its service when contracted through a telephone carrier. According to the contract with Vivo, the service is governed by both companies' terms of use. However, the terms of use for Vivo's customers to subscribe to Prime Video do not mention the protection of the data of those who acquired the service. They only refer to the forms of engagement, the method of payment, and the service cancellation. The information on privacy and security related to the mobile or broadband plans is available on Vivo's Privacy Center website.[62] However, there is no specific information on the Amazon Prime Video service.

In Amazon Prime Video's terms of use, available through a hyperlink on the contract with Vivo, customers will also find a link to Amazon's Privacy Notice and Advertisement Notice; however, these are in English. In other words, only with an investigative insistence would consumers find the privacy policies of Vivo and Amazon, and, in the case of Amazon, they would have to know English to understand it, even though the service is offered in Brazil and in partnership with a company established in this country. These circumstances prevent informed consent and hinder the consumers from accessing information or controlling the use of data.

In addition to this difficulty in accessing the applicable privacy policies, knowing who the controller companies are and the type of data processed, Vivo's Privacy Policy and Amazon's Privacy Notice open the possibility for more actors to access the data of their consumers. However, if we assume that consent concerning the processing of data by these companies is barely informed to the user, the situation is even worse when it comes to data shared with third parties.

When answering the question: "Does Amazon share your personal information?" Amazon's Privacy Notice states that "we are not in the business of selling our customers' personal information to others," but mentions the actors with whom it shares data. These include what the Privacy Notice calls "affiliated business we do not control," but does not specify who are these affiliates, as the text only refers to another text that mentions some examples, namely American, such as Starbucks, OfficeMax, Verizon Wireless, Sprint, T-Mobile, AT&T, J&R Electronics, Eddie Bauer,

62. https://www.vivo.com.br/portalweb/appmanager/env/web?_nfls=false&_nfpb=true&_pageLabel=vivoVivoInstPrivacidadePage&WT.ac=portal.amarca.privacidade&# (el servicio ya no existe).

and Northern Tool + Equipment. It could be assumed that Vivo would also be in this category. Finally, the Privacy Notice also states that, when buying or selling Amazon business, "Customer information generally is one of the transferred business assets," but states that it remains subject to the privacy policies preceding the sale. All these provisions open up massive gaps for us to question the principle of purpose and consumer consent to use their data.

For its part, iFood states that the "members of the iFood group" and "service providers and other partners" may have access to customer data.[63] The policy is vague and does not specify which data might be shared, even suggesting that the company may outsource iFood services to its subsidiaries, and consequently, its user base. It also states that it only shares data with third parties for marketing purposes when said third party has privacy protection patterns similar to those of iFood, but does not detail precisely what types of data may be shared. Therefore, it is impossible to evaluate whether these data would be necessary for marketing purposes or to extrapolate said purpose. In any case, the policy is not specific nor comprehensive and seems to open a wide window to the possibility of accessing to the service's user base.

For its part, Magazine Luiza has a relatively lax privacy policy concerning obtaining its users' consent. The document only mentions the use of the data and the customer's future possibility to unsubscribe from the marketing email database. It makes no mention to obtaining prior, informed, and consented authorization to the processing of data. Regarding shared data, the privacy policy states that "user data will not be shared, sold or presented to third parties who are not its partners."[64] Just like the other cases mentioned here, Magazine Luiza's policy continues being vague. It does not mention who its eventual partners might be nor whether it will share data for marketing purposes.

3.2.2. Use of Cookies

Besides sharing data with third parties, the four companies state that they use cookies and various web trackers. Contrary to the provisions of the General Data Protection Regulation (GDPR), the Brazilian law has no specific provisions on the use of these technologies. However, we can raise the question of how the use of cookies and similar tracking technologies

63. iFood, "Privacy Policy," 2018.

64. "Política de Privacidade," 2015, *Magazine Luiza*.

could be reconciled with the principles of purpose, suitability, necessity, and even non-discrimination, all of which are contemplated in the Brazilian law.

Of the companies analyzed, only Social Miner has a dedicated cookie policy, something expected considering that the start-up's services are primarily based on tracking cookies for marketing campaigns. This policy explains what they are and what types of cookies are used by the company.

Social Miner's privacy policy quotes the GDPR to state that the start-up adheres to the European regulation. The presence of such a statement is commendable. Nevertheless, the policy states that Social Miner's client is responsible for informing the users of the use of cookies and the collection of personal data (in the case of a connection via email or social media sites). This is understandable from an operational perspective, but makes the user vulnerable, as it depends on the client's (Social Miner's contracting party) transparency patterns.

In turn, iFood specifies that information about user activity on the website or the company's application is aggregated and considered as "non-personal" data since it supposedly does not allow identifying each user. The policy also states that "the age, preferences, language, CEP and the area code" of a user are "non-personal data."[65] Such classifications may indicate an attempt to exclude such information from legal protection. They refer to data that is clearly personal and that, without proper processing, can easily be used to identify specific individuals. Hence, iFood's willingness to classify specific data as non-personal is dangerous and opens a door for a potential violation of the customers' privacy.

Regarding the use of cookies to collect data of the users by the services studied, note that these data serve as identifiers created or collected regarding a user. By adopting the concept of "information regarding an identified or identifiable natural person,"[66] it can be said that the LGPD considers that cookies act as an electronic identifier (Gomes 2018) or that they have the purpose of inferring purchase profiles as a means to collect personal data.

Furthermore, iFood's privacy policy states that "in some of our email messages [iFood uses] a 'click-through URL' (external address) linked to

65. iFood, "Privacy Policy," 2018.

66. Government of Brazil, Presidência da República, 2018, "Exposição de Motivos da Medida Provisória 869/2018." http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Exm/Exm-MP-869-18.pdf

iFood's content. Whenever customers click on one of these URLs, users are directed to a different server before arriving at our services' destination website. iFood monitors click-through data to understand the interest in specific subjects and evaluate the efficiency of the communication with our clients" (Gomes 2018). In case the client does not wish to be monitored, the policy requires that he/she "does not click on the text or the links contained in email messages sent by iFood" (Gomes 2018).

Apparently, customers are not notified of the user routing to the servers before the destination website—except to those who read the entire privacy policy before clicking on any link iFood sends to its customers via email. Such a practice is not ideal and may violate users' rights to consent to the collection of their data.

In the case of Magazine Luiza, the application's privacy policy contains a specific section on cookies, providing that the website/application may use them and that the user may disable them. The document explains that product recommendations will be made by a cookie that identifies the user's browsing activities. In this case, browsing encompasses the user's behaviour within the website/application by focusing on factors such as 1) whether the user only browsed or purchased a product; 2) items seen, searched, or bought; 3) other users in similar situations.[67]

Amazon's Privacy Notice also deals specifically with cookies by mentioning the possibility of disabling them from the browser. However, at the same time, it states that "if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Services that require you to sign in." So, although it is possible to disable cookies, it is impossible to do so and continue using Amazon services. Note that there are different types of cookies with different functions, so it would be technically possible to distinguish them and enable only those necessary for the platform's operation.

3.2.3. Can the Relationship with GAFAM Occur Under Unauthorized Processing of Sensitive Data?

Regarding sensitive personal data, which the law defines as "personal data concerning racial or ethnic origin, religious beliefs, political views, trade union or membership to a religious, philosophical or political organization, data concerning health or sex life, genetic or biometric data, when related to a natural person" (Article 5, section 2), the LGPD even states

67. "Política de Privacidade," 2015, *Magazine Luiza*.

that "anonymized data shall not be considered personal data […] except when the process of anonymization to which the data was submitted has been reversed, using its own means exclusively, or when it can be reversed applying reasonable efforts." In other words, the processing of data that does not lead to identifying the subjects has a more significant window of exploration.

The relationship between the companies studied and the GAFAM companies, and therefore with other databases, open the door to access their clients' sensitive data. However, none of the privacy policies studied explicitly mention the processing of these data, although many engage in profiling activities.

3.2.4. Right to Easy Access, Correct, or Delete Information

The LGPD also guarantees the subject the right to easily access the information about the purpose of the data processing, its duration and form, information about the data controller, and the data shared with third parties.

Social Miner's privacy policy contains provisions about the information shared with third parties and the purpose of the data collection. However, there is no clarity on how long the user's data is stored and no provisions describe how they may request corrections or the deletion of data from their base.

For its part, iFood states that it may store the data for as long as required for the effects of the privacy policy and to comply with the terms of use, "respecting the data retention period determined by the applicable legislation."[68] It also states that the users may request the exclusion of the account but does not mention how to make such a request. In any case, it provides that:

> In some cases [iFood may] retain your information, even if you have deleted your account, such as in the case of mandatory record-keeping under applicable law, when there is an unresolved issue regarding your account (such as, for example, an unresolved complaint or dispute), or as necessary for our legitimate business interests, such as fraud prevention and improving the security for our users.[69]

68. "Política de Privacidade," 2015, *Magazine Luiza*.

69. iFood, "Privacy Policy," 2018.

The retention of data for legitimate business interests opens an arena for many possibilities considering the ambiguity of the term used and can lead to excessive and abusive storage for users. Furthermore, as mentioned in the policy, customers' feedback on iFood deliveries may be used for advertisement purposes and may be posted on the platform's website and application. However, it is not known whether there is clarity for users in terms of the unrestricted visibility of their feedback beyond the provisions of the privacy policy.

Magazine Luiza considers the user a de facto data subject and allows the user to add, delete, or correct the information linked to their user profile.[70] Although the document provides a guarantee of the user's right to access, correct, or delete their information, it does not mention how to do so. On this point, the privacy policy does not address the possibility of data exclusion following the end of the relationship that led to its collection, nor does it mention the processing period of the user's personal data.

In the case of Amazon Prime Video, the Privacy Notice mentions that you may enter account information for the "limited purpose of displaying it" and, in some cases, updating it. The document also states that some examples are available, but the link provided redirects to the Privacy Notice. Again, one is apprehensive about the fact that the streaming service does not have a specific privacy policy, since the profiling process for a video streaming service is different, for example, from the profiling done for buying or selling products.

Consider cases such as the one pointed out by a New York Times article (Fisher and Taub 2019) that, when investigating the YouTube recommendations and search system in Brazil, showed that the platform tends to direct users toward far-right-wing channels. Therefore, it is necessary to think about what kind of transparency can be demanded from this and other types of streaming services that increasingly use artificial intelligence to make recommendations. Finally, there is no explicit mention of the possibility of data exclusion.

3.2.5. Profiling and the Algorithm's Discriminating Potential

The LGPD is not very clear in regard to profiling practices. Article 5 of the law provides definitions of personal data, sensitive personal data, and anonymized data[71] and describes that data anonymization is the use of

70. "Política de Privacidade," 2015, *Magazine Luiza*.

71. For purposes of this Law, the following definitions apply:

"reasonable and available technical means at the time of the processing, through which data loses the possibility of direct or indirect association with an individual." Furthermore, the law authorizes the processing of personal data by research entities to conduct studies, ensuring, whenever possible, the anonymization of personal data (Article 7(iv)).

Another critical point is that the LGPD does not consider anonymized data as personal data unless the anonymization process can be reversed.[72] Article 12 also states that data can be considered personal when used to formulate behavioural profiles of a particular natural person if that person is identified, and that the national data protection authority may provide for "standards and techniques to be used in anonymization processes and perform security checks."

In that sense, if profiling practices work with anonymized data, these do not represent a violation of the LGPD. Furthermore, the law does not define the "reasonable efforts or its own means" (Soares 2018) applicable to anonymization reversal processes or the minimum standards for companies.

I – personal data: information regarding an identified or identifiable natural person;

II – sensitive personal data: personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person;

III – anonymized data: data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing;

72. Article 12: Anonymized data shall not be considered personal data, for purposes of this Law, except when the process of anonymization to which the data were submitted has been reversed, using exclusively its own means, or when it can be reversed applying reasonable efforts.

§1 The determination of what is reasonable shall take objective factors into account, such as cost and time necessary to reverse the process of anonymization, depending on the available technology, and the exclusive use of its own means.

§2 Data can be considered personal, for purposes of this Law, when used to formulate behavioral profiles of a particular natural person, if that person is identified.

§3 The national authority may provide for standards and techniques to be used in anonymization processes and carry out security checks, with opinions from the National Board for the Protection of Personal Data.

Generally speaking, concluding whether the activities of the companies analyzed in this study influenced the profiling practices or the eventual discriminations caused by algorithmic decisions was impossible.

iFood's privacy policy claims that the company classifies its clients according to their actions. For instance, it classifies users who "order a specific category of food more or make more than four orders a month."[73] However, the specific and particular uses of such classifications, which may result in vulnerabilities for users to the extent that they provide clear parameters of personal preferences and habits, are unknown.

Social Miner's operations, in turn, are based on the automatic analysis of the user's purchase behaviour made by the start-up's algorithm. However, there is no indication of how such an algorithm works and of the potential categorizations of users into groups according to purchase patterns, which again leaves the user vulnerable and potentially overexposed. The company claims that it conducts studies on consumers' patterns. In this case, "Such data will have the users' personal information deleted, which is no longer considered personal data, but as a mere set of anonymous data for study and research purposes."[74] Even so, it indicates that there is, to some extent, some profiling based on user data.

MagaLu's Privacy Policy also disregards possible profiling practices by the company and the content routing or customer clustering strategies. The document only refers to the possible use of cookies that identify the user's browsing for the subsequent recommendation of products that will be differentiated depending on the behaviour on the website. The document also mentions that the product recommendations will "be generated by algorithms, the accuracy of which may not be exact; however, it will procure suggesting products that are relevant to the user, without it having any obligation to acquire them."

Amazon Prime Video hired data analysis experts to enhance its algorithms. However, its terms of service and privacy policy do not say much about how it works or how users can intervene. Especially because the privacy policies are generic and apply to all Amazon services and not specifically to Amazon Prime Video. The specific policy only mentions the software, stating that it may provide Amazon with:

---

73. iFood, "Privacy Policy," 2018.

74. "Política de Privacidade" (no date).

> Information related to your use and the performance of the service and the software, as well as information related to the devices on which you download and use the software service. For example, the software may provide Amazon with information regarding the digital content you download or *stream* and your use of that digital content (such as whether and when you viewed the digital content, which may, among other things, help us measure the period of access to the digital content you rent).[75]

However, there is no information on how these data are used or whether the consumer may directly edit the profile that Amazon attributes to him.

3.2.6. Other Matters Covered by the LGPD

Furthermore, the law contains a specific provision on the processing of children's and adolescents' personal data. According to the LGPD, this processing requires the specific consent given by one of the parents or legal guardians. This does not apply "when [the] collection is necessary to contact the parents or the legal guardian," used "one single time and not stored, or for their protection, and under no circumstances shall the data be passed on to third parties without their consent" (Article 14, paragraph 3).

Bearing in mind the importance of paying attention to the international transfer of data, since many Internet resources and applications transit through very diverse countries and legislations, the LGPD states that such transfer is only allowed "to countries or international organizations that provide a level of protection of personal data that is adequate to the provisions [of the] law," and "when the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided [in the] Law" (Article 33, paragraphs 1 and 2). In other words, the Brazilian law follows the standard set by the European regulation (GDPR), only allowing the transfer to countries with a data protection standard similar to Brazil's.

Specifically, regarding the controllers and processors, that is, those who are responsible for the decisions on the processing of personal data and those who potentially perform it on behalf of the controller, the LGPD states that both must maintain records of their operations to

---

75. Amazon Privacy Notice, 2017: https://www.amazon.com/gp/help/customer/display.html?nodeId=468496

maintain a report of the data processing. This report shall contain at least "a description of the types of data collected, the methodology used for collecting data and for safeguarding the security of the information, and the analysis of the processor regarding the adopted measures, safeguards and risk mitigation mechanisms" (Article 38, paragraph).

In the case of patrimonial, moral, individual, or collective damages arising from the processing of personal data, the controllers and/or processors have the obligation to compensate the users according to the judicial measures. Furthermore, the law provides that "the processor is jointly liable for the damages caused by the processing when it does not comply with the obligations of the data protection legislation or when it has not followed the controller's lawful instructions" and that "controllers who are directly involved in the processing from which the damages to the data subject arise shall be jointly liable" (Article 42, paragraph 1, (I) and (II)) even when the damage results from the neglect of any of them regarding the adoption of adequate security measures.

4. Evaluation of the National Data Protection Authority's Capacity to Deal with CDBBMs

The Brazilian National Data Protection Authority (ANDP) was created according to Law 13.583 dated July 8, 2019, 11 months after the enactment of the General Data Protection Law. However, the model of Personal Data Protection Authority adopted by Brazil is far from being the one desired by some sectors involved in the discussion of the law, since the entity will be part of the direct public administration and will be attached to the Civil House of the Presidency of the Republic.

Note that the discussions around the LGPD in the National Congress involved an independent authority model, with decision-making, institutional, and financial autonomy, capable of implementing and supervising the application of the law. The legality of the creation of the ANDP as an autarky was broadly questioned, as the specificities of the model were added to the text of the law during the legislative debate. The arguments around the illegality in the creation of the ANDP during the discussion of the law influenced on the Executive Power's decision, which considered that the National Congress was violating the exclusive competence of the Presidency of the Republic to legislate on the organization of the Direct

and Indirect Public Administration, and eventually vetoed the provisions related to the ANDP.

However, on December 27, 2018, Provisional Measure n. 869/2018 was published,[76] which, upon being enacted as Law 13.853/2019 amended the Data Protection Law and reintroduced the provision creating the ANDP as a federal public administration body attached to the Presidency of the Republic in the text of the LGPD, recognizing that the vetoes represented a "risk of legal insecurity for the Civil Society given the lack of definition of the body responsible for the regulation, control, and monitoring of the law's application."[77]

The functions of the authority are defined in Article 55-J[78] which, to summarize, are: a) monitor the compliance with the data protection law; b) monitor and apply penalties; c) resolve the requests of data subjects (citizens) against the controllers; e) prepare studies; f) foster the adoption of privacy-friendly services; g) cooperate with the data protection authorities of other countries; h) request reports and make arrangements to publicize processing operations; i) conduct studies and amend

---

76. Congresso Nacional, Medida Provisória n. 869/2018. https://legis.senado.leg.br/sdleg-getter/documento?dm=7966761&ts=1563991644604&dispositi on=inline

77. Government of Brazil, Presidência da República, 2018, "Exposição de Motivos da Medida Provisória 869/2018." http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Exm/Exm-MP-869-18.pdf

78. The most relevant include a) ensure the protection of personal data under the terms of the law [...] c) develop guidelines for the National Privacy and Data Protection Authority; d) monitor and apply the appropriate penalties in the event of data processing performed in breach of the law, using the administrative proceeding concluding otherwise, the broad defense and the right to appeal; [...] f) disseminate the knowledge of the data protection public policies and regulations, and the security measures, among the population; g) promote and prepare studies on the protection and privacy national and international practices [...]; i) Promote international or translational cooperation actions with the data protection authorities of other countries; [...] m) Edit data protection and privacy regulations and procedures, as well as reports on the impact to data protection when data processing poses a high risk to guarantee the general data protection principles outlined in this Law; [...] q) edit simplified and differentiated regulations, guidelines, and procedures, even regarding the deadlines for the micro and small businesses, as well as incremental or disruptive corporate initiatives declaring themselves as startups or innovation companies may adhere to this Law; s) discuss, strictly and in the administrative, the interpretation of this Law, its competences, and omissions.

regulations; j) perform audits or determine their performance; and k) communicate breaches to the competent authorities.

The ANDP is responsible for preparing the National Privacy and Data Protection Policy guidelines, monitoring the data processing activities, and applying the appropriate penalties to the actors who breach the rights provided in the law. The following duty was included during the legislative debates:

> Publishing simplified and differentiated regulations, guidelines, and procedures—including the deadlines—for micro and small businesses, as well as incremental or disruptive corporate initiatives declaring themselves as start-ups or innovation companies, to adhere to this law.[79]

The legislator tried to provide for a kind of staggered application of the law for start-ups and disruptive companies. Therefore, the challenge for the ANDP is to define the regulations and deadlines for its adoption by start-ups to balance the right to privacy and data protection with the promotion of innovation without undermining the recently conquered legal regime.

Article 52 of the Law provides the sanctions applicable to agents responsible for data processing (I—warning, indicating the time period for adopting corrective measures; warning, simple fine, daily fine, blocking, and deletion of the personal data). These do not replace the application of administrative, civil, or criminal sanctions in the specific legislation.

Despite the importance of creating a Data Protection Authority, the institutional arrangement for the exercise of supervisory power is not ideal. This was noted by Bruno Bioni in an interview with *Jornal O Estado de São Paulo.* For example, the veto to the possibility of applying administrative sanctions to data processors regarding the:

> (a) Partial suspension of the operation of the data bank to which the sanction refers for a maximum period of six (6) months, which may be extended for an equal period until the controller regularizes the processing activity; (b) Suspension of the exercise of the personal data processing activity to which the sanction refers for a maximum period of six (6) months, which may be extended for the same period; and (c) Partial or total

79. Law 13.853/2019.

prohibition of the exercise of activities related to the processing of the data.[80]

According to the law's text, the application of the administrative sanctions described above will only occur in the event of a repeat offence by a given company or public administration entity. In other words, the application of the provisions could only occur after the imposition of at least one of the administrative sanctions described in the list of Article 52 or, in the case of controllers, subject to other bodies and entities with sanctioning powers, once these bodies issue their decision.

Note that the sanctions described above were fundamental to strengthen the National Data Protection Authority and vest monitoring and control power in it, becoming a robust authority, with reinforced sanctioning power and relevance to prevent abuses committed by data processors and controllers. However, it can be said that the Brazilian authority model will be insufficient, since the body is constituted devoid of autonomy. The law guarantees the technical and decision-making autonomy of the data protection authority; however, its financial and institutional autonomy are still pending an eventual revision.

The size of the ANDP is also quite modest, consisting of a governing council comprising 5 members and a National Data Protection Council comprising 23 members. However, the structure of the ANPD is still unknown insofar as the law only states that the body shall have an oversight office, an audit office, a legal advisory team of its own, and any administrative units and specialized units necessary to enforce the law (Article 55-C).

The authority proposed was enhanced through the creation of the National Data Protection Council (CNPD) (Article 58-A). This multisector body, comprising 23 representatives of the public, private, and civil sector—and academia—allows for more active participation of the sectors interested in the activities of the ANPD. According to the Law (Article 58-B), the duties of the CNPD include: 1) preparing strategic guidelines and providing subsidies to develop the National Privacy and Data Protection Policy and the actions of the ANPD; 2) preparing annual

80. Brazil's National Congress, 2019, Medida Provisória n. 869/2018: https://legis.senado.leg.br/sdleg-getter/documento?dm=7966761&ts=1563991644604&disposition=inline

evaluation reports on the implementation of the actions of the National Privacy and Data Protection Policy; 3) preparing studies and conducting public debates and hearings; and 4) disseminating knowledge.

With regard to the issue of autonomy and independence of the ANPD, the countermeasure found and added to the text was the inclusion of two paragraphs to the law, which indicate that the Executive Branch may transform the legal nature of this body into an autarky, and that this endorsement must occur within a period of up to two years after August 2020 (the effective date of the Law).[81]

Conclusion and Recommendations

Generally speaking, the known practices by CDDBMs were identified in the companies analyzed. The use of cookies and other methods to collect browsing data, share databases with third parties, and content routing in platforms via profiling were identified—one way or another—in the companies analyzed in this study. Furthermore, as in the case of Colombia, there is a strong relationship with the GAFAM companies, whether due to the use of data of the platforms for user authentication, or the possibility of content routing in them.

In regard to the four companies analyzed, the current privacy policies of iFood and Magazine Luiza were written before the enactment of the LGPD and, therefore, do not explicitly mention the law or their obligations under it. Similarly, Social Miner does not mention the LGPD but makes explicit references to the European regulations, stating that it follows the European standard. Regarding Vivo, which makes Amazon Prime Video available, the company recently launched a Privacy Center which, in one way or another, adheres to the principles of the LGPD, but most of the service's data are governed by Amazon's Privacy Notice, which does not mention the Brazilian law and is only available in English.

---

81. Article 55-A: Create, without further expenditure, the National Data Protection Authority (ANPD), an entity of the federal public administration attached to the Presidency of the Republic.
§1 The legal nature of the ANPD is temporary, and the Executive Power may transform it into an indirect entity of the federal public administration, subject to a special autarkic regime and associated to the Presidency of the Republic.
§2 The evaluation of the transformation mentioned in §1 of this article shall occur during a period of up to 2 (two) years from the effective date of the ANPD's regulatory structure.

If we take into account the legal regime presented and the current situation of the national data protection authority, it is still too early to suggest that the regulation will be strong enough to tackle possible violations of privacy and citizens' rights by the companies. Under the approved model, the National Data Protection Authority is weak and lacks adequate monitoring power. Based on this, for the monitoring to be effective in the country, the body must be willing to cooperate with other sectors and inspection bodies such as those belonging to the National Consumer Defense System and the Federal Justice itself.

Therefore, we recommend the following:

To the analyzed data processors:

To update their privacy policies and terms of use to be consistent with the General Data Protection Law. The companies need to adhere to the Brazilian law, both in the terminology and in their actions, seeking to make the rights guaranteed by law and the details of the processing of their personal data clearer to the user. Social Miner's policy, for instance, falls short. It mentions the European regulation several times in its policy privacy but fails to mention the Brazilian law that will soon apply throughout the country.

To disseminate their privacy policies and terms of use in a relaxed and integrated way, translating them into Portuguese. For example, there were difficulties in understanding which privacy policy governed Amazon Prime Video's services when hired through Vivo. It is essential that companies provide clear, sufficient, and easily accessible information to their customers or potential customers—as required by law—and, if two companies are involved, developing a single document explaining to the consumer the role of each company in the processing of his or her data would be essential.

To disseminate and include mechanisms and/or contact information for the users who wish to receive more information regarding the processing of their data in the terms of use and privacy policies. Although the LGPD provides the possibility for users to request information or amendments on the processing of their data, this possibility is still uncertain in the policies analyzed, and a large part of the CDDBMs believe that the user will take a clear path whenever they wish to use their rights under the LGPD.

To implement governance policies. None of the four companies analyzed had guidelines aimed at governance measures or principles to guide data processing and maintain users' security. The LGPD recommends that companies be transparent regarding their internal data management processes, but so far, the companies analyzed do not show a clear implementation of such a recommendation.

To obtain details on the security measures adopted by the companies. Some companies used vague terms to refer to the subject; others even disclaimed their responsibility of compensating the users in the event of leaks or breaches.

Further research on the actions of CDDBMs in the country based on their impact on citizens' rights and freedoms is required. Especially considering the imminent application of the law, both users and the companies must provide policies on the relationship between the rules on data protection and the companies' actions in Portuguese and explicitly tailored to the Brazilian context. Such studies may even be used by the ANDP once it starts operating, building technical and empirical knowledge on the subject.

The use of cookies and other trackers should also be understood and analyzed with further detail so that the data they collect is not interpreted as being anonymized by default and, therefore, outside the scope of the protection of the law, as could be seen in some of the privacy policies.

Sometimes, it should be noted that sensitive data is being collected as part of the relationship with GAFAM companies. However, no mention to sensitive data was found in any of the privacy policies.

Also, that the standard for certain data collections should be the opt-in, as opposed to the opt-out, which was common to the terms analyzed.

Finally, there must be more clarity and transparency on the companies' profiling practices. It is an issue that was not clearly mentioned in any of the privacy policies or the terms of use.

Regarding the National Data Protection Authority:

To review the National Data Protection Authority's transformation model—as provided in the law—and its subsequent transformation into an autarky attached to the Indirect Public Administration, with technical and financial autonomy and with robust monitoring power to safeguard the users' rights and apply more severe sanctions to the controllers.

To override President Jair Bolsonaro's vetoes on the text of MP 869/2019 to restore the more severe sanctions included in the course of the legislative debate to strengthen the authority policing power (suspensions) and making it financially independent.

References

Belloni, Luiza. 2018. "Como o iFood se tornou o maior aplicativo de delivery de comida da América Latina." *Huffington Post*, April 18, 2018. https://www.huffpostbrasil.com/2018/04/18/como-o-ifood-se-tornou-o-maior-aplicativo-de-delivery-de-comida-da-america-latina_a_23414651/

Brigatto, Gustavo. 2018. "Movile investe US$ 500 milhões no iFood e planeja criar líder global." *Valor Econômico*. https://www.valor.com.br/empresas/5983273/movile-investe-us-500-milhoes-no-iFood-e-planeja- criar-lider-global

Calado, Caio. 2018. "Magazine Luiza : entrevista com o time responsável pela criação da Lu." Medium Bots Brasil. https://medium.com/botsbrasil/magazine-luiza-entrevista-com-o-time-respons%C3%A1vel-pela-cria%C3%A7%C3%A3o-da-lu-8fc987fbafad

Daroit, Guilherme. 2019. "iFood quer seguir entregando crescimento." *Jornal do Comércio*, May 27, 2019. https://www.jornaldocomercio.com/_conteudo/cadernos/empresas_e_negocios/2019/05/685035-ifood-quer-seguir-entregando-crescimento.html

Fisher, Max, and Amanda Taub. 2019. "How YouTube Radicalizes Brazil." *New York Times*, August 11, 2019. https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html

Fraga, Nayara. 2018. "'Temos de ajudar o consumidor na inclusão digital,'" diz Trajano, do Magazine Luiza." *Época Negócios*. https://epocanegocios.globo.com/Empresa/noticia/2018/02/fabio-coelho-do-google-e-luiza-trajano-do-magazine-luiza-conversam-sobre-inclusao-digital.html

Freitas, Tania. 2019a. "As 8 startups brasileiras de machine learning que serão aceleradas pelo Google." *Startse*. https://www.startse.com/noticia/startups/61939/8-startups-brasileiras-launchpad-accelerator

Freitas, Tainá. 2019b. "iFood registra 17,4 milhões de pedidos no mês de março." *Startse*. https://www.startse.com/noticia/startups/63248/iFood-atinge-a-marca-174-milhoes-de-pedidos-n o-mes-de-marco

Gartenberg, Chaim. 2019. "YouTube is Back on the Fire TV, and Prime Video Launches on Chromecast Starting Today." *The Verge*, July 9, 2019. https://www.theverge.com/2019/7/9/20686773/youtube-fire-tv-prime-video-chromecast-amazon- google-launch-today-available

Gazeta do Povo. 2017. "iFood e Magazine Luiza estreiam sistema de pagamentos online do Google no Brasil." *Gazeta do Povo*. https://www.gazetadopovo.com.br/economia/nova-economia/ifood-e-magazine-luiza-estreiam-sistema-de-pagamentos-online-do-google-no-brasil-24pqsn32pbqozn86seh3ktp7i/

Gomes Oliveira, María Cecilia. 2018. "Cookie notice: informar, obter e por fim coletar dados pessoais." *jota*. https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/cookie-notice-informar-obter-e-por-fim-coletar-dados-pessoais-23112018

Higa, Paulo. 2019. "Fim da briga: YouTube volta ao Fire TV e Prime Video estreia no Chromecast." *Tecnoblog*. https://tecnoblog.net/297901/youtube-volta-fire-tv-prime-video-chromecast/

Jesús, Aline. 2012. "Magazine Luiza lança F-commerce no Facebook e Orkut." *Techtudo*. https://www.techtudo.com.br/noticias/noticia/2012/02/magazine-luiza-faz-sucesso-com-seu-f-commerce-no-facebook-e-orkut.html

Letieri. 2019. "Usuários colocam iFood no sobrenome e não conseguem mudar." Techtudo. https://www.techtudo.com.br/noticias/2019/05/usuarios-colocam-ifood-como-sobrenome-no-facebook-e-nao-conseguem-mudar.ghtml

Luna, Denise. 2018. "MP do DF abre inquérito contra Vivo por suspeita de uso de dados pessoais." *O Estado de S. Paulo*. https://link.estadao.com.br/noticias/empresas,mp-do-df-abre-inquerito-contra-vivo-por-suspeita-de-uso-de-dados-pessoais,70002253400

Magazine Luiza. 2019. "E-commerce do Magazine Luiza cresce 56% no segundo trimestre Em menos de três anos, faturamento do Marketplace chega a ¼ das vendas digitais." Press Release. *Magazine Luiza*. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiW8r-W7YntAhVBFlkFHV9JA8cQFjAAegQIBxAC&url=https%3A%2F%2Fri.magazineluiza.com.br%2FDownload%2Fmagalurelease2T19--1-%3F%3DIart1882KdnmVEwBwRdEmQ%253D%253D%26idcanal%3DrqFYRysdRDkT

GGc93mpXJg%253D%253D&usg=AOvVaw1BqHQO-IjCJmxX-jI4_APfb

Manzoni, Jr., Ralphe. 2017. "Como o Magazine Luiza pretende enfrentar a Amazon?" *Istoé Dinheiro*. https://www.istoedinheiro.com.br/como-o-magazine-luiza-pretende-enfrentar-amazon/

Meio and Mensagem. 2018. "Amazon Prime Video e Viacom anunciam conteúdo original." *Meio and Mensagem*. https://www.meioemensagem.com.br/home/ultimas-noticias/2018/11/14/viacom-negocia-series-para-amazon-prime-video.htmll

Monteiro, R. L. 2017. "Proteção de dados e a legislação vigente no Brasil." Baptista Luz. http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf

Oracle. 2018. "New Start-ups Join Oracle Start-up Cloud Accelerator to Enhance Cloud Innovation." https://www.oracle.com/br/corporate/pressrelease/startup-accelerator-brazil-second-cohort-2018-06-07.html

Privacy International. 2019. "State of Privacy Brazil." https://privacyinternational.org/state-privacy/42/state-privacy-brazil

Ricciardi, Alex. 2016. "Como Frederico Trajano está mudando os rumos do Magazine Luiza." *Forbes*. https://forbes.uol.com.br/negocios/2016/07/como-frederico-trajano-esta-mudando-os-rumos-do-magazine-luiza/

Soares Campos, Pedor Silveira. 2019. "Anonimização na Lei Geral de Proteção de Dados requer posição da ANPD." *Conjur*. https://www.conjur.com.br/2019-mar-10/pedro-soares-anonimizacao-lei-geral-protecao-dados#_ftn3

Souza, B. 2016. "Como a Social Miner usa inteligência artificial, mas também gente, para inovar no marketing digital." *Projeto Draft*. https://projetodraft.com/como-a-social-miner-usa-inteligencia-artificial-mas-tambem-gente-para-i novar-no-marketing-digital/

Veloso, Thássius. 2012. "Magazine Luiza lança programa de comissão para Facebook." *Tecnoblog*. https://tecnoblog.net/74606/magazine-luiza-facebook/

Zuini, Priscila. 2013. "Movile investe R$ 5,5 milhões na iFood." *Exame*. https://exame.com/pme/movile-investe-r-5-5-milhoes-na-ifood/

ACCOUNTABILITY OF FACEBOOK AND OTHER BUSINESSES IN CHILE: PERSONAL DATA PROTECTION IN THE DIGITAL AGE

Paloma Herrera
Pablo Viollier

The objective of this report is to evaluate the preparedness of the Chilean legal regime to address the new dynamics of the digital age and its capacity to hold companies with a data-driven business model (CDDBM) accountable.[82]

To this end, this report will be divided into five sections. In Section 1, we select four CDDBMs and describe the criteria to choose said companies as representative of four categories: 1) large Internet companies; 2) intermediate companies; 3) start-ups; and 4) established companies. We will characterize and evaluate four companies in this paper: Facebook, PedidosYa, AIRA, and Falabella.

In Section 2, we describe and evaluate the operations of these CDDBMs. This characterization will be based on a study of the distinct terms and conditions of the selected companies' products and will revolve around four analysis categories: 1) source of data processed; 2) processing performed; 3) purpose of the processing; and 4) relationship with Google, Amazon, Facebook, Amazon, and Microsoft (GAFAM).[83]

---

82. Throughout this report, the CDDBMs are understood as those companies with a "business model that relies on data as a key resource" (Hartmann et al. 2014, 6).

83. Note that this report will evaluate the business model of these four particular companies; therefore, the conclusions we may reach regarding them are not necessarily applicable to other companies of the same market segment or with a similar business model.

In Section 3, we aim to evaluate the preparedness of the Chilean data protection legal regime to address the new dynamics of the digital age. Specifically, this analysis will be divided into two parts. First, we will study the activities or dynamics of the digital age and of the companies selected that are inadequately regulated by the national data protection law. Second, we analyze the territorial scope of application of the data protection regulation and its extraterritorial application to the CDDBMs studied.

For this, we analyze the contents of Law N° 19.628 on the protection of privacy and other national regulations governing the collection, processing, and storage of personal data.[84] Since Chile is undergoing a legislative reform of its data protection regulations, we will compare the regulations currently in force under Law N° 19.628 and those proposed in the bill that regulates the protection and processing of personal data and creates the Personal Data Protection Agency (2017), currently under discussion. Finally—and where relevant—we will use the European Union General Data Protection Regulations (GDPR) as benchmark to evaluate the relevance and level of protection of the regulations studied.

Section 4 addresses the mechanisms to enforce the data protection law. Specifically, we seek to determine whether the habeas data procedure, contained in Law N° 19.628 (of a judicial nature), provides sufficient safeguards to comply with the law, exercise the data subjects' rights, and the legal system's capacity to hold the CDDBMs accountable.

Finally, we make preliminary recommendations to improve the Chilean legal system's capacity to face the challenge of the new dynamics of the digital age and business driven by the processing of personal data.

1. Methodology

The methodology used in this report is based on a review and analysis of the privacy policies and terms of use published by the CDDBMSs on their websites, as described in Annex 1 of this report. Furthermore, we complement the research with information obtained from media statements issued by the CDDBMs about their operations and business methodology. The analysis also includes a study of the national regulation, specifically Law N° 19.628, and the amendments being discussed, as well as the provisions of the GDPR.

84. Ley N° 19.628, "Sobre protección de la vida privada," Ministerio Secretaría General de la Presidencia. August 18, 1999. https://www.leychile.cl/Navegar?idNorma=141599

To complete this analysis, we held a focus group on October 4, 2019. Eleven representatives of the industry, civil society, technical community, public entities, and legal offices specialized on the subject attended this meeting. The remarks made by the participants of the focus group are transcribed to complement the analysis of the legal regime to compile the opinions of the actors participating in the debate around data protection in Chile.

2. Selection of CDDBMs

Although the systemic storage of data by corporations and public entities is usual practice in the 21st century, the evolution and proliferation of information and communication technologies (ICTs) has impacted how CDDBMs process and manage data. The main characteristic CDDBMs share, regardless of their size, volume, or how consolidated they are in the market, is that they process data or use the information they obtain to innovate and create new products. This way, companies focus their actions on using this information to attract more customers and users to their respective businesses (Diaz and Zaki 2015).

Within the national context, a report prepared by International Data Corporation (IDC 2018) predicts that 60% of the expenditure on IT by companies for the 2019–2020 period will be invested in technologies such as cloud computing, big data, Internet of things (IoT), and Artificial Intelligence (AI) to improve their productivity and cut their expenses. In turn, regarding AI, a study conducted by Technology Visio 2019 (Accenture Technology Vision 2019) showed that 46% of Chilean executives surveyed said that their organization has adopted AI, whereas 29% claim the same worldwide (TrendTic 2019).

We selected four CDDBMs to describe and analyze the Chilean situation, considering their consolidation in the Chilean market and classifying them into four categories: 1) large Internet companies, 2) intermediate companies, 3) start-ups, and 4) established companies.

2.1. Large Internet Companies

For this category, we selected Facebook Inc. as one of the companies grouped under the acronym GAFAM (Google, Amazon, Facebook, Apple, and Microsoft), known for its dominant position in the information and technology market. We selected this company because it has 2.271 billion active users worldwide (We Are Social and Hootsuite, 2019), and over

13 million users in Chile (Montes 2018). Facebook is also an ideal company to analyze for this report because its business model revolves around collecting and processing personal data (including sensitive data) to profile its users and sell personalized advertising to its clients.

For this report, we note that while Facebook Inc. offers a variety of products and services, most notably the Instagram social networking service and the WhatsApp instant messaging service, we will limit our description and analysis solely to the terms of use and privacy policies for the Facebook social networking site.[85]

In this context, these companies' concentration power and dominant market position concern various sectors of society. The Cambridge Analytica scandal, which involved collecting and processing a high number of personal data shared through the social network Facebook, is well known. In the end, Facebook signed a settlement with the United States Federal Trade Commission (FTC) and agreed to pay a USD $5 billion fine as a result of various irregularities detected in its privacy system (DW 2019).[86]

2.2. Intermediate Companies

In this category, we chose the company PedidosYa, an online delivery company with headquarters in Uruguay and a presence in various Latin American countries. The company has been operating in Chile since 2010 and has one of its main offices in the country. To choose this company, we searched the ranking prepared by the applications market and information company App Annie,[87] considering the most popular applications in Chile from Apple's App Store and Google Play, according to the index for the first five days of June 2019.[88]

Several companies provide online delivery services for products and services in Chile, including food delivery applications such as PedidosYa,

---

85. "What are the Facebook Products?" (no date). Retrieved July 25, 2019, from https://www.facebook.com/help/1561485474074139?ref=tos.

86. For more information on the settlement between Facebook and the FTC, visit the following link on Facebook's website: https://about.fb.com/news/2019/07/ftc-agreement/

87. Top App Matrix, 2019. For more information on the App Annie platform refer to the following website: https://www.appannie.com/dashboard/home/

88. Although on the initial methodology document we considered studying the months of April, May, and June 2019, App Annie only provided free access to the information collected in the last 30 days; therefore, to access the information for previous periods, we had to either pay a fee or link the personal iTunes or Google Play user accounts, which we considered excessive processing of data.

Rappi, and UberEATS. However, PedidosYa, the pioneer in Chile in providing these services, has had the largest growth and has the broadest coverage in over 20 cities, from Arica to Puerto Montt.[89]

These applications' business model is based on e-commerce, allowing users to access various products and services offered through a virtual platform. The operation of these platforms are based on serving as an intermediary between the consumer, the restaurant, and the order's distributor by charging a commission for the use of the platform[90] and the intermediary service to all the transaction's participants.

According to the website, the intermediation service these apps offer in the food industry has the following advantages: 1) access to a new sales channel, 2) optimization of the delivery system, 3) no fixed costs—charges only according to the orders received, 4) customized online menu, and 5) corporate commitment by PedidosYa.[91]

At a national level, the use of these applications has also resulted in increased sales for food products in general. The Department of Studies of the National Chamber of Commerce, Services and Tourism (CNC 2019) reported that fast food sales recorded real annual growth of 5.4% during the first quarter of 2019, reflecting the influence of the increased use of delivery apps throughout the country.

2.3. Start-ups

To select the company for the start-ups category, we considered the initiatives of the economic and sociocultural sector that use the scientific and technological knowledge enabled by the intensive use of the Internet to build their business model on data (Vega and Ramírez 2018), have an innovative business model, and have been created recently. Therefore, we selected the Chilean company AIRA (Artificial Intelligence Recruitment Assistant), which offers artificial intelligence software that recruits, selects, and validates the background of candidates to short-term jobs by using Big Data and Artificial Intelligence.

---

89. More information is available in Spanish on the application's website: www.pedidosya.cl

90. A tax modernization bill that establishes a tax on digital services is currently being discussed by the Congress. If passed, the costs to implement and use these applications would increase (Chile, Chamber of Deputies, 2018).

91. "Nosotros" (no date). Retrieved July 25, 2019, from https://www.pedidosya.cl/about/beneficios-restaurantes

AIRA began operating in the country in 2016 and is currently used by over 30 companies of the financial, retail, and construction sectors. What makes this start-up interesting, and the reason why we chose it, is that—on its website and various media—it mentions that it is capable of building rankings of up to one thousand resumes in a matter of seconds, identifying the professional experience of candidates by using biometric technology.[92]

According to this start-up's CEO (Nava 2018), AIRA operates as follows:

- Classification of candidates and submission of a set of questions previously prepared by AIRA to the profiles considered suitable for a specific position. Once the applicants answer these questions, the system analyzes their answers and creates a shortlist.
- According to the results provided by AIRA, the applicants shortlisted for the next stage would go on to a "virtual interview," classifying their emotions and gestures as positive, negative, or neutral.

AIRA mentions that the effectiveness of its process lies in the fact that the system is designed not to discriminate by sex or age, so the recruitment process would be expedited both for the company and the applicants, thus avoiding the uncertainty of traditional interviews.

The company has been recognized in various global contests in the United States, Switzerland, and Chile. It won Corfo's National Innovation and Entrepreneurship Olympics, was chosen in the Top 10 most innovative Chilean technology companies by SeedStars World, and was contacted by the company Y Combinator, a start-up accelerator from Silicon Valley in the United States.

2.4. Established Company

For this category we chose Falabella, a company whose operations precede the enactment of Law N° 19.628. Falabella[93] is a retail company founded in 1889 in Santiago de Chile. The company has expanded its business to other Latin American countries (Colombia, Peru, and Mexico) as it has

---

92. The use of biometric technology implies a series of risks and possible violations of people's rights. For an in-depth study, see Becker and Garrido (2017).

93. For more information, visit the About Us section (in Spanish) on the company's website: "Quiénes somos" (no date). Retrieved July 25, 2019, from https://investors.falabella.com/Spanish/quienes-somos/default.aspx#section=about

managed to maintain an agile business model, with a substantial injection of resources in technology and innovation. For instance, Grupo Falabella acquired 100% of the virtual store Linio,[94] one of the leading marketplaces of the region.

Falabella is currently considered one of the leading e-commerce companies. It successfully adapted by changing its business model—initially based on a scale-efficiency economy—to a client-driven model and the customization of its products and services. Therefore, Falabella has stood out for investing large amounts of money in technology. This year, the company has focused on leveraging its growth by specializing its logistics centres using Big Data and AI.

3. Characterization of CDDBMs Operations

To describe and analyze how CDDBMs operate in the country, we classified the information contained in their privacy policies into four categories of analysis: 1) data sources, 2) processing, 3) purpose of data processing, and 4) relationship with GAFAM.

3.1. Data Sources

Law N° 19.628 refers to the term "source" only to classify personal data processed according to the public or private nature of the place where they were collected, regardless of whether the information was provided by the data subjects. However, for the effects of this section, we considered "data source" as that which derives from 1) information provided by the user, 2) third-party data, and 3) data obtained through monitoring, e.g., web tracking.

3.1.1. Information Provided by the User

During sign-up, the four CDDBMs ask the user for minimal data such as their email address, date of birth—to verify the minimum age required to use these services—and a password as access control.

On the requirement of a password to access the services, we note the case of Falabella. On its website, the company mentions that signing up with an account associated to a password is optional: "This password is not a requirement to hire our services, but it allows personalized,

94. Linio operates in eight countries including Mexico, Colombia, Peru, Argentina, and Chile, and has offices in the United States and China. See Linio, "SACI Falabella informa adquisición del 100% de Linio y anuncia aumento de capital," (no date): https://www.linio.cl/sp/linio-grupo-falabella

confidential and safe access."[95] However, it provides no further details on why browsing or making transactions through a registered account is safer or more confidential than a purchase without signing up, considering that Falabella must comply with a hypertext transfer protocol secure (https). The reason for this statement is neither explained nor inferred and could be interpreted as a form to disincentive purchases without signing up.

On the contrary, AIRA, Facebook, and PedidosYa require signing up to access their services.[96] However, only PedidosYa explains said requirement in its privacy policy: "We provide you with a username and a password, enabling you to access restricted areas of our website or other contents and services."[97]

Facebook[98] and Falabella require additional and excessive information during sign up on their respective sites, including a person's "sex." Asking for information on gender is considered excessive because, upon analyzing the purpose of collecting and processing these data—which is no other than facilitating the creation of an account on the social networking site—any information that allows identifying the user through a username and a means for contact should be enough. The requirement to provide information related to the user's identification with a specific sex for signing up is unjustified. This ignores that not all users identify with a gender, in which case the sign-up process requires information that is considered sensitive data under the national laws. Although Falabella's request for sex-related information is optional, Facebook[99] defends the mandatory provision of information on sex and the option of indicating gender, arguing that it will be used to send personalized messages (Her: Wish her a happy birthday; Him: Wish him a happy birthday), without providing further information on the matter.

---

95. Emphasis added. For more information (in Spanish), visit "Tu cuenta" (no date): https://www.falabella.com/falabella-cl/page/comprar-terminos-condiciones?staticPageId=37900007&menu=comprar&srv=c5

96. Note that Facebook allows accessing specific text posts, videos, and images that users made public without requiring the visitor to have an account.

97. "Términos y condiciones" (no date). Retrieved July 25, 2019, from https://www.pedidosya.cl/about/terminos-condiciones

98. Facebook asks for the user's "sex"; however, during sign up, it provides the option "non-binary gender."

99. Consider that, in the case of Facebook, the inclusion of information concerning gender is indicated as optional.

In the case of AIRA, the site only asks for an email address and an access password. However, it also offers the option of linking Facebook and Google accounts, but provides no further information. Moreover, the only terms and conditions referring to privacy and data protection available on the portal are addressed to job applicants, in a brief and general way:

> PRIVACY PROTECTION: APPLICANTS using AIRA's SERVICES enjoy all the privacy rights mentioned in Chilean Law N° 19.628 on the Protection of Privacy and Personal Data, and may especially exercise the rights to access, revoke, change and update their personal data, including their email address, and to object to the processing of their data according to the provisions of said law.[100]

Besides the data needed to sign up, the other data sources collected from the user will depend on the type of business developed by the CDDBM.

Therefore, companies focused on direct sales (Falabella) and intermediation (PedidosYa) of products also collect information related to the products selected on the shopping cart, shipping address, amount, and payment method. The above can be seen in their respective privacy policies. While Falabella indirectly refers to the above by defining personal data as the "name, RUT, address, telephone number, email address, geolocation data, website use, and visits, browsing history, purchase habits, among others," PedidosYa mentions that it collects data on "your visits and use of this website, including your IP address, geographic location, type of browser, source of reference to the site, duration of the visits and number of visits per site."[101]

However, none of them explicitly refers to said data sources. Likewise, in the case of Falabella, this company even classifies this type of information as personal data and not as sensitive data, being that, under the national law, the latter should receive a higher standard of protection for the simple reason that it reveals personal habits of the user through the website.

Unlike Falabella and PedidosYa, the social networking site Facebook provides greater detail and transparency about the processing of these

---

100. AIRA, "Condiciones de uso para postulantes," 2019: https://shared-files.airavirtual.com/terminos-postulantes

101. "Términos y condiciones" (no date).

data by mentioning that, whenever a user makes a transaction through their site, the processing includes "payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details."

In the case of AIRA, which offers recruitment and personnel selection assistance to its clients, its privacy policy provides little detail regarding other sources of information. However, upon studying the different sections of AIRA's website, we found that their additional data sources include those obtained from the resume uploaded by the applicant, the psychometric test, and the video interview, also called Emotion Analytics.[102]

Since this is sensitive information under the law, these data deserve an explicit mention in the website's privacy policy. Especially to meet the objective of making the processing activities more transparent and explaining how said information is collected and stored to ensure that the data subjects are unequivocally consenting to the processing of these data.

3.1.2. Data Created by Monitoring

After analyzing the four CDDBMs, we concluded that data is monitored mainly through web tracking[103] to profile a user and his or her behaviour patterns.

In the case of Falabella and PedidosYa, although both companies focus on electronic commerce in different areas (retail and food delivery, respectively), users' usual behaviour is to browse through the various options of products and services to meet a specific need. In both cases, the information collected revolves around purchases, potential purchases, and browsing habits to offer personalized offers to users and induce them to consume specific products.

---

102. This tool measures the emotions transmitted by the applicant when answering the questions, influencing the contracting decision by the employer. The use of these tools has been controversial, and it has been pointed out that it is impossible to identify emotions from facial expression since a person's behavior varies greatly depending on the specific and sociocultural context. Nor is it possible to avoid the discrimination bias because a human initially classified the expressions. Other risks to privacy and data protection arise if there is no clarity on the source of these data, their collection, or how they are stored (Feldman et al. 2019).

103. Practice to identify devices, browsers, and tools usually used by Internet users. Its purpose is to obtain and use this data to correctly collect, classify, and compile information to profile a user and his or her behavioral patterns.

In the case of Facebook, from an ordinary user's perspective, he or she uses the platform for entertainment and social interaction purposes. Therefore, the information collected in this area refers to the contacts (friends) and companies (sites) that the users follow and with which they interact on the social media site. Based on the collection of these data, these are analyzed and provided to the brands that wish to advertise themselves on the site, which allows defining specific audiences to promote their products or services.

For its part, AIRA does not provide further information on this subject, but Falabella, PedidosYa, and Facebook refer to the data they collect through monitoring in their respective privacy policies. Thus, Falabella generally notes the use of analytical cookies: "At Falabella, we use cookies and similar technologies to personalize and enhance your customer experience and to show you relevant online advertising." On the other hand, in its cookies section, PedidosYa describes with more detail that they use analytical, session, and persistent cookies by stating that they collect "information about your computer and about your visits to and the use of this website including your IP address, geographic location, browser type, referring sites, length of visits and number of page views."[104]

Facebook is the company that best describes its monitoring methods. It categorizes the data obtained according to the mechanisms used: 1) device attributes, 2) device operations, 3) identifiers, 4) device signals, 5) data from device settings, 6) network and connections, and 5) cookie data.[105]

3.1.3. Third-party Data

For this section, we will consider the data obtained from strategic partners or third parties. In this case, only Facebook's privacy policy and terms of use refer to third-party data as follows:

> We also receive and analyze content, communications, and information that other people provide when using our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information.[106]

---

104. "Términos y condiciones" (no date).

105. "Data policy" (no date). Retrieved July 25, 2019, from https://www.facebook.com/about/privacy/update

106. "How does Facebook work with data providers?" (no date). Retrieved July 25, 2019, from https://www.facebook.com/help/494750870625830?ref=dp

As well as information provided by their so-called, "partners."

Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plugins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook.[107]

However, it is noteworthy that Facebook indicates that for third parties to provide the information, they require each of these third parties to have lawful rights to collect, use, and share your data.[108] In contrast, AIRA does not inform the data it collects from third parties in its policy or terms of use. This is disturbing considering their business model is based on the data they must provide to the companies contracting their personnel recruitment services.

3.2. Data Processing

Law N° 19.628 defines "data processing" as any operation or set of operations or technical processes—automated or not—that allows collecting, storing, recording, organizing, devising, selecting, extracting, confronting, interconnecting, dissociating, communicating, assigning, transferring or cancelling personal data, or its use in any other way. As shown above, the Chilean law provides an extremely vague definition of data processing, which covers practically any relevant activity on personal data.

For the effects of this research, we will limit the study to two of the essential elements recognized by the legal definition provided above in the context of the CDDBMs analyzed: 1) collection and 2) analysis of data.

3.2.1. Collection

The technology used by CDDBMs to collect data is web tracking, specifically through cookies, as noted in the previous section.

Facebook, Falabella, and PedidosYa refer to the use of cookies in their respective policies and terms of use. However, these mentions vary in the specificity and level of information provided.

---

107. Ibid.

108. Ibid.

In the case of Falabella, the company makes a generic reference to analytical cookies. It points out the use of *similar technologies* to customize the advertising and services displayed to a given user. However, it provides no further detail on what "similar technologies" mean. PedidosYa emphasizes on the type of cookies it uses, explaining the use of session and persistent cookies as follows:

We will use persistent cookies to enable our website to recognize you whenever you visit our site. Session cookies will be deleted from your computer once you close the web browser. Persistent cookies will be stored in your computer until deleted or until the set expiration date.[109]

In the case of Facebook, as mentioned above, it has a dedicated cookies policy—just like Falabella—which refers to the use of "other technologies" without providing further information on the matter, mentioning that, for the effects of that policy, they will be considered as "cookies," without explaining the limits or scope of such statements.

Although, unlike PedidosYa, Facebook does not classify the type of cookies it uses, it makes a detailed description by providing examples of their functions. Hence, without explicitly mentioning them when referring to the personalization cookies for advertisement purposes, Facebook provides the following examples:

> We use cookies to count the number of times an ad is shown and calculate the cost of those ads. We also use cookies to measure how often people do things like click on or view ads.[110]

For its part, AIRA makes no mention of cookies or other technologies to collect data. However, we found that upon analyzing the source code of all the websites associated to the CDDBMs, AIRA, and PedidosYa's website—which provides information on the cookies it uses, from the category to the duration of the cookies—use the Hotjar tool, the use of which is not specified in any of these websites' policies.

Hotjar is a data analysis suite used in digital marketing. It combines various data collection and analysis features into a single platform. In this context, it is noteworthy that its main features include the creation

---

109. PedidosYa, "Términos y condiciones" (no date). Retrieved July 25, 2019, from https://www.pedidosya.cl/about/terminos-condiciones

110. Similarly, Facebook has dedicated sites on each type of cookies (https://www.facebook.com/policy/cookies?list) and a general cookies policy (https://www.facebook.com/policy/cookies).

of "heatmaps" (records of users click on a website) and the possibility of recording user sessions on the website (monitoring user recordings to observe what they are doing).

The use of Hotjar is a clear example of how cookies are used for advertisement purposes and how data on browsing habits is stored. So, the omission of this information on the privacy policies can violate the users' expectations of privacy[111] when browsing on the CDDBMs' websites. In the case of PedidosYa, although it fails to refer to the use of Hotjar, it is the only one whose terms and conditions explicitly mention the use of Google Analytics to create statistical information on the use of the website through cookies.

In turn, although Facebook does not mention the algorithms or analytical tools it uses, it refers to its collaboration with certain data providers such as Acxiom, Oracle Data Cloud (formerly DLX), Epsilon, Experian, and Quantium, where the third party using the services of these data providers provides said information to Facebook.[112]

3.2.2. Analysis

CDDBMs collect data to process and channel them to create information with great corporate value and identify consumption patterns or optimal customer loyalty strategies. This allows companies to meet the user's needs and create a business strategy to optimize the services according to the user's behaviour.

Concerning the analysis, it is usually descriptive and aimed at segmenting the users and audiences according to their abilities, tastes, interests, and connections; or prescriptive, understanding this concept as what should happen to improve the user's experience in the future visits.

From a descriptive perspective, both Fallabella and Facebook mention, in their privacy policies, that they analyze data to segment their users and personalize the content and/or products offered. Thus, in summary, Facebook mentions that it analyzes data to suggest communications with other users, Facebook pages, and relevant ads, depending on the GPS location. On the other hand, Fallabella mentions that it analyzes data to

---

111. Concept developed in the U.S. used by the North-American jurisprudence to evaluate the limits of privacy in each specific case (Saldaña 2001).

112. According to a 2019 announcement by Facebook, third parties' access to certain information will be limited under the settlement reached with the United States FTC ("Cleaning up data access," Facebook Newsroom: https://about.fb.com/news/2019/07/cleaning-up-data-access/)

prepare, advertise, and offer new products and services and so that the user may enjoy the benefits of the CMR PUNTOS loyalty program.[113]

In the case of AIRA, regardless of the vagueness of its privacy policy, the information provided by the applicants to the work positions offered by the companies who hire AIRA's services is standardized and classified according to the company's requirements. In this regard, AIRA mentions that:

> AIRA's responsibility: a) provide SERVICES in a correct, timely and complete manner, so that all APPLICANTS are considered for the recruitment processes defined by the COMPANY but performed by AIRA's technology in an objective and standardized form, thus providing equal opportunities to all APPLICANTS to provide and convince the COMPANY of their affinity with the job offer.[114]

For its part, PedidosYa does not refer to this issue. The company merely states that:

> Any user may use PedidosYa services provided it is included within the following defined groups: anonymous user; any Internet user; Registered user: Any user that previously registered for free on the basic data site.[115]

Regarding the prescriptive analysis, whose purpose is to improve the user's experience, the CDDBMs merely refer to data processing for this purpose instead of providing further information or describing the automated tools and systems they use to analyze data.

3.3. Purpose of Data Processing

The principle of purpose is considered as the cornerstone of all the regulations governing personal data processing. Data should not only be collected following the legal standards, but it must also be used for the purpose for which it was collected. Any person may process personal data provided they do so according to the law and for the purposes allowed.

---

113. "Tu cuenta" (no date). Retrieved July 25, 2019, from https://www.falabella.com/falabella-cl/page/comprar-terminos-condiciones?staticPageId=37900007&menu=comprar&srv=c5

114. AIRA, "Condiciones de uso para postulantes," 2019.

115. PedidosYa, "Nosotros" (no date). Retrieved July 25, 2019, from https://www.pedidosya.cl/about/beneficios-restaurantes

Processing data for purposes other than those authorized by the data subject or not authorized by the law is illegal.

CDDBMs have multiple reasons to collect personal data, including providing a service, creating user profiles, and analyzing the consumer's behaviour. All these purposes must be informed and consented to by the user before the collection and processing.

Consequently, purposes have been classified into three categories: 1) to use the products, 2) for content personalization, and 3) to communicate with the user.

AIRA makes a vague reference to the purposes of its processing by stating that "AIRA may only use the proprietary [sic] INFORMATION of the APPLICANT in regard to the SERVICES subject to these CONDITIONS," describing that the purpose is to provide compiled personal data to the company who hired AIRA's AI services to recruit personnel.

In the case of Falabella and PedidosYa, we note that they provide information on the purpose of its data processing by employing a list that is easy to understand for the user. Thus, Falabella mentions that, additionally, its related companies may process personal data in general to personalize content and to sell their products and services to the customer/user:

> Your personal data may be processed by Falabella and/or its Related Companies, on its own or through its vendors, only to (i) prepare, implement, promote and offer new products and services to you or new attributed, modalities or features of the products and services already available to you; (ii) automatically fill the documents related to the transactions you make regarding the products acquired and/or the services used or hired, or acquired, used or hired in the future, with Falabella or its Related Companies; (iii) access and process your data to adjust our offer of products and services to your customer profile or to make analysis, reports or evaluations on the matter; and (iv) develop general or personalized commercial actions or post-sale services to improve your experience as a customer.

On the other hand, PedidosYa mentions that it may use personal information to:

> i) manage the website, ii) improve the website's personalized browsing experience, iii) enable the user to use the services available on the website, iii) [sic] send general commercial communications, iv) send email notifications requested explicitly by

the user, and v) send our newsletter and other communications related to the website we believe will interest you, and which you explicitly agreed to, via email.

However, regarding the last item, in PedidosYa, the box where the user agrees to receive advertisements and other information is checked by default. This is regrettable since it is widely known that users do not read the conditions of use or privacy policies and quickly accept all terms and conditions to use the services, thus inadvertently authorizing several types of processing for advertising purposes. Although this conduct cannot be classified as illegal, it does constitute a bad practice, since the doctrine's consensus is that the consent of the data subject must always be informed, express, and specific.

Finally, in the case of Facebook, the social networking site broadly mentions that "to provide the Facebook Products, we must process information about you," but fails to provide a clear list of purposes that is easily accessible by the user. In fact, only the user who can devote sufficient time to read the various documents comprising Facebook policies and general conditions may understand these purposes, which are spread all over the social networking site.[116]

3.4. Relationship with GAFAM

All the companies that base their business in data models are related to Google, Amazon, Facebook, Amazon, or Microsoft in one way or another. All these companies interact through the sites Facebook offers to companies for advertisement purposes and from the interoperability of their platforms (metrics, analysis, and other corporate services).[117]

Considering the presence of companies through Facebook pages, Falabella, AIRA, and PedidosYa have official Facebook sites to create

---

116. For example, when referring to the source of data collection, in the section on the collection of biometrical data through the camera, Facebook mentions that their purpose is to "do things like suggest masks and filters that you might like, or give you tips on using camera formats." However, another section indicates other purposes where it is inferred that the data collected could be used either for research or advertising purposes, to name a few examples.

117. "Por qué es mejor crear una página en Facebook," Facebook for Business, 2014: https://www.facebook.com/business/news/LA-Por-que-es-mejor-crear-una-Pagina-en-Facebook-para-tu-negocio

advertisements, be a direct communication channel with their users, and create advertisements within the site.[118]

Regarding the interoperability of Facebook with other companies—which should be understood as a system's capacity to work and relate to other existing systems—special consideration should be given to the case of PedidosYa, since it allows users to register by linking their Facebook account.[119]

When the potential PedidosYa user chooses this form of registration, he or she automatically provides the company with access to the information stored on Facebook, which may be considered somewhat excessive considering the user's motivations—quick registration on the site—and the purposes of PedidosYa to process these data (delivering products sold by third parties). This is verified by checking the "How PedidosYa can use your information" section of Facebook, which simply states that "PedidosYa can use the information you provide to personalize your experience and connect with your friends."

The latter is worrisome and contrary to the principle of purpose. If compared to the Facebook terms and conditions, they point out that by linking an application (e.g., PedidosYa) to a Facebook account, the application is granted permission to access information contained in Facebook, such as age, language setting, gender, and even the list of friends, who are third parties that have not explicitly given their consent. Given the above, PedidosYa should explain the limits and consequences of signing up by linking accounts more clearly, either by making it explicit on its portal or by referring the user to the specific section of Facebook's policies covering conditions of use of this type of data.

---

118. "Your Ad Preferences" (no date). Retrieved July 25, 2019, from https://www.facebook.com/ads/preferences

119. In this regard, in 2019 Facebook announced the creation of "Off-Facebook Activity" platform within Facebook that allows the user to see and control the data applications and websites shared with Facebook. However, as of the writing of this report, this platform is not available for users in Latin America ("Now You Can See and Control the Data that Apps and Websites Share with Facebook Newsroom": https://about.fb.com/news/2019/08/off-facebook-activity/)

4. Capacity of the Personal Data Protection Legal Regime

Law N° 19.628 on the protection of privacy was enacted on August 18, 1999. It is one of the first laws to regulate data protection in the region. However, even before its publication, this law was described as insufficient to protect data subjects from the processing performed by third parties (Jijena 2001).

Today, there is a consensus among experts, academia, and civil society around how the law is inadequate to appropriately protect personal data (Comité de Evaluación de la Ley 2015). This deficient level of protection is explained by the course of the years and because its elaboration was strongly influenced by particular interests. The law's legislative discussion was marked by the significant participation and lobbying of representatives of the industries interested in exploiting personal data, to the detriment of the influence exercised by academia and civil society. As Jijena (2010) mentions, Law N° 19.9628 was drafted "under the direct advice of groups, associations, and companies interested in ensuring the business of personal data processing, compounded to the insufficient knowledge of the congressmen who promoted it." Therefore, it is possible to assert that the objective of the law was to offer a regulatory framework for the database market rather than create a system to protect the informational autonomy and data subjects' rights from a fundamental rights perspective.

The main flaws of the current law include:

> [...] the absence of effective sanctions, the lack of regulation of the cross-border flow of personal data, the authorization of the use of data for direct marketing without the consent of the data subject, the lack of registration of private data banks, the absence of a public control authority, broad exceptions to consent for data processing, and the lack of adequate procedural safeguarding mechanisms (Viollier, 2017, p. 4).

The impetus to modify and update the Chilean personal data regulations has been determined by two factors. First, the commitment Chile acquired upon joining the Organization for Economic Cooperation and Development (OECD) which consists in implementing the Guidelines related to the protection of privacy and the cross-border flow of personal data (OECD 2002) and, to a lesser extent, by commitments related to the right to privacy and the cross-border flow of personal data

with the Asia-Pacific Economic Cooperation Forum (APEC), although these provide a less robust protection scheme than the OECD guidelines (APEC 2005; APEC 2009). Second, Chile's desire to increase its level of protection and achieve the status of adequate legislation following the standards set out in the European Union's General Data Protection Regulation.

Chile has embarked on two significant reform processes. First, the amendment of Article 19 (4) of the Constitution, which raised personal data protection to the constitutional sphere. Currently, this provision reads as follows:

> The Constitution guarantees all persons [...] 4. The respect and protection of private life and the honour of the person and his family and, similarly, the protection of their personal data. The processing and protection of these data will be carried out in the form and under the conditions determined by law.

Second, the bill will regulate the protection and processing of personal data and create the Personal Data Protection Agency, presented on March 15, 2017, to increase the personal data protection standard and comply with the OECD's requirements on the matter.

In the following sections, we will analyze the aspects of the current law that do not regulate or deficiently regulate the digital age activities as performed by the CDDBMs analyzed in the preceding section.

4.1. Regulatory Gaps

4.1.1. Inferred Sensitive Data and Data from Which They Are Inferred

Article 2(g) of Law N° 19.628 defines sensitive data as follows:

> [...] personal data that refers to the physical or moral characteristics of a person, or facts or circumstances of their private life or privacy, such as personal habits, racial origin, ideology, and political beliefs, religious beliefs and convictions, physical or mental health status, and sexual life.

The law defines the category of sensitive personal data without specifying how this data is obtained. In this sense, a systematic interpretation of the legislation leads us to conclude that the database controller must comply with the additional requirements that the category of sensitive personal data entails, regardless of whether the data is obtained with the

consent of the owner or through automated processing that allows inferring sensitive data.

This is particularly relevant concerning the business model of some of the CDDBMs studied. It is precisely inferred data that allows profiling users to know their purchase history and offer them personalized products or know their personal habits and deliver targeted advertising.

This interpretation makes sense when taking into consideration the legal nature of the link between the subject and his or her personal data. The condition of subject, as opposed to other forms of legal ties such as domain or ownership, implies that the subject cannot waive, assign, or dispose of his or her control over the data relating to his or her person (Contreras 2019). In the same sense, the subjects are entitled to exercise their right to access, rectify, cancel, or object their personal data, even if these have been inferred by the database controller through algorithmic or automated mechanisms. Unfortunately, Chile has no case law on this issue, leaving it relatively open to interpretation and generating legal uncertainty for individuals' rights.

The Personal Data Bill does not mention inferred data in any of its articles. Article 9 of Gazette No. 11.144-07 regulates the right to personal data portability, establishing that database controllers must provide a copy of the personal data concerning the subjects in a structured manner and in a generic and commonly used format, which allows it to be operated by different systems as requested.

However, Article 9(a) of the bill states that "this right may not be exercised in respect of information inferred, derived, created, generated or obtained from the analysis or processing carried out by the controller." This section would be justified because allowing the portability of inferred data would create a problem in the personal data processing market, allowing any competitor to access information generated or inferred through private mechanisms and that is protected under trade secret or copyright. However, the limitation on inferred data only extends to the exercise of the right of portability. Therefore, the subjects of personal data would be fully entitled to exercise all the rights on inferred data granted by the law, including the right of access, and the processing of this type of data must meet the same requirements as data obtained through other mechanisms that enable the processing of personal data and sensitive personal data.

Finally, the fact that the current definition of sensitive data mentions personal habits as an example provides interpretative elements to

conclude that the behaviour, routine, and other aspects of the subjects' intimate life are expressly protected by the law. In this sense, the profiling of users and their personal habits is often done through data inferred from background information such as their purchase, browsing, or location history, which would fall within the current definition of sensitive personal data. This discussion is relevant because an express mention of personal habits as sensitive personal data was removed during the debates of the bill in the Senate Constitution Committee, a clear step backward from the current protection standard (CIPER 2019).

Consequently, a meaningful discussion arises regarding the legality of the use of cookies by the companies studied. If the personal habits (among which we can consider web browsing) are sensitive data, then its processing requires express consent from the data subject.[120] However, whether the inclusion of the use of cookies among the terms and conditions accepted by the user meets the requirement for express, informed, and specific consent is debatable.

On the other hand, the fact that the broad definition of personal data contained in the Chilean law allows the subject to maintain control over the data that platforms such as Facebook infer on him or her, initiates a meaningful discussion: the possibility for data subjects to exercise their ARCO rights concerning this non-transparent assessment made by the platform based on his or her online behaviour. For example, if the platform processes the data of a given user and classifies them as a person with conservative political opinions, this information must be considered sensitive, as it is related to the subject's political views. This way, the data subject should have the means to gain access to this evaluation and rectify it if it is incorrect, outdated, or inaccurate.

In this regard, a participant of the focus group from the industry sector mentioned that he felt it was important for "definitions to be as broad and flexible as possible," and that the definition of "sensitive data is fine as a list, but should not be strict." Similarly, another expert on the matter said that "the important thing is that the definitions can be adapted. The authorities and the courts are responsible for interpreting it under the light of the new technologies and forms of processing."

120. Article 10 of Law N°. 19.628 provides an exhaustive list of situations in which a third party will be authorized to process the subject's sensitive data: 1) with the subject's consent, 2) under legal authorization, 3) in the case of data required to determine or provide health benefits to the subjects.

On the legal status of the inferred data, a representative of a public entity, whose duty is related to the protection of personal data, had an opinion similar to that presented in this report and said that:

> [...] inferred data is an issue; there is also observed data and personal data. The answer is not simple; even in Europe it has not been solved. Chile has the advantage of considering personal habits as sensitive data, which may be applied to inferred data. One can say that the inferred data is an opinion or a consequence of legal analysis (it is probabilistic).

4.1.2. Internet Protocols (IP) and Similar Identifiers and Data Associated With Them.

Article 2(f) of Law N° 19.628 defines data of a personal nature or personal data as those "related to any information on identified or identifiable natural persons." This definition is relevant as it establishes the scope of application of the law: it is only applicable to the processing of personal information.

For this analysis, the possibility that a piece of information may be considered personal because it refers to or is linked to a determinable person is relevant. According to Cerda (2012, 16), data can be considered personal when it allows identifying someone by using "the set of means that may be reasonably used by the data controller or any other person to identify the individual." This way, although the law does not explicitly refer to the IP address as personal data, one could interpret that it constitutes personal data to the extent that it is accompanied by other information that allows identifying a specific individual (geolocation data, web tracking, among others).

On the other hand, the only legal provision that specifically refers to the IP address is Paragraph five of Article 222 of the Criminal Procedure Code, which provides the obligations for telecommunications companies to maintain, "An updated list of its authorized IP addresses ranges under reserve and at the disposal of the Public Ministry, and a record, of at least one year, of the IP addresses of the connections made by its subscribers." Therefore, it is a general metadata retention scheme whose constitutionality is questionable given the disproportionate nature of the measure and the impact on the population's right to privacy (Canales and Viollier 2018).

Hence, this is a borderline case that requires clarification on whether the IP address may be linked to a particular person during a case. The

Supreme Court of Chile has referred to the possibility of data being personal when it may be associated to a specific individual. This way, in the ruling of Case N° 2479-2018, the Court ruled that vehicle license plates could be considered personal data, holding that a report filed during a lawsuit:

> [...] included the image of an Audi vehicle without removing or distorting the part of the picture showing the license plate, thus allowing any person who watched the show to identify the vehicle's owner and, eventually, associate him with the contents of the story through minimum search efforts.

This way, the Court seems to establish a "minimum search effort" test. In contrast, Recital 26 of the European Union General Data Protection Regulation (GDPR) provides that "[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."

The Council for Transparency had a similar opinion in case C-611-2010, where it expressly referred to the nature of the telephone number as personal data, stating that:

> [...] from the perspective of personal data protection, considering that the telephone number is associated or can be associated to the name of a natural person, said information constitutes personal data; therefore, those processing it are obliged to keep it secret when this data is acquired or has been collected from non-publicly accessible sources.

The fact that data can be considered personal if it can be associated with a specific individual with minimum effort has also allowed arguing that—within the framework of a mass request for information by the regulator to telecommunications companies—the mobile phone number can be considered as personal data if it is accompanied by other data that allows profiling the customer (Canales 2019). The European law has used similar reasoning to consider the IP address of a device and the email address (even when it does not coincide with the name of the account holder) as personal data.[121]

---

121. Among others, refer to Judgment C-582/14 of the Court of Justice of the European Union.

To summarize, there is sufficient background in the Chilean law and jurisprudence to argue that the IP address can be considered as personal data if it can be associated with a specific individual by other means. However, the legislation should provide clear guidelines for interpreting this specific case. Therefore, the fact that the bill does not explicitly refer to the IP address and the cases in which it could be considered as personal data is concerning. However, Article 2(f) of the bill defines personal data as:

> any information related or referring to an identified or identifiable natural person. An identifiable person shall include any person whose identity can be determined, directly or indirectly, by *information combined with other data*, in particular through an identifier, such as an identity card number, analysis of elements specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that person, excluding cases disproportionate identification efforts. (emphasis added)

Thus, the mention to information combined with other data provides additional tools to interpret the cases when data can be associated with an identifiable person.

This statement is contained in the recitals of the bill and would not constitute a binding rule. However, it serves as an element to consider when interpreting the scope of the IP address as data that can be considered personal if it can be associated with a specific person.

This is relevant because the analysis of the companies contained in the previous section shows that the use of cookies allows collecting the IP address as data. Out of the companies studied, only PedidosYa expressly mentions the IP address although it is not difficult to imagine that the other companies that use cookies also collect it. More in-depth research would be necessary to find out what type of use is given to the IP address, whether the companies cross-reference this information with other data that allows identifying the user using the IP address and whether the companies—considering the IP address as personal data—take the necessary safeguards concerning its processing or, on the contrary, they consider it as statistical information.

4.1.3. Profiling

The four CDDBMs studied build their value offer on user profiling, whether to offer personalized services or products, advertisements to specific demographic segments, or recruit personnel. One could argue that

user profiling is at the heart of the business model of many of the leading Internet giants, including GAFAM. This poses a significant challenge in terms of regulations, considering that profiling has the potential of violating the fundamental rights of data subjects, whether due to the power asymmetry between the user and the platform, the eventual tracking and monitoring of the activities required to perform it, and the behaviour customization or manipulation it may cause (Büchi et al. 2019).

Law N° 19.628 does not explicitly regulate the creation of profiles or profiling of data subjects. However, the fact that personal habits are considered sensitive personal data provides interpretative elements to argue that the data obtained through profiling falls within this category and, therefore, is protected. This means that their processing is subject to additional requirements.

This is an issue addressed by the personal data bill currently under discussion. One of the provisions of the bill presented by the executive branch in July of 2018 amends Article 2(w), which defines profiling:

> [...] as any form of automatic processing of personal data consisting of the use of such data for evaluating, analyzing, or predicting any aspect of a natural person's professional performance, financial situation, health status, personal preferences, interests, reliability, behaviour, location or movements.

This inclusion enables a more accurate characterization of a core activity in the business model of many online platforms. However, the articles do not consider profiling results as sensitive personal data; on the contrary, in the bill, this definition is reduced to:

> [...] personal data that discloses the ethnic or racial origin, political views, membership to a union, ideological or philosophical convictions, religious beliefs, data related to health status, human biological profile, biometrics, and information related to the sex life, sexual orientation and gender identity of a natural person.

Similarly, the elimination of personal habit as sensitive personal data makes it harder to interpret that data resulting from profiling enjoys the highest level of protection, so the bill compromises the level of protection provided by the current law (CIPER 2019).

For its part, Article 4(4) of the GDPR defines profiling as:

> [...] any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

This definition is nearly identical to that contained in the Chilean bill and shows the influence of the European regulation. Similarly, the GDPR mentions profiling regarding the right to object, particularly the right not to be subject to decisions based exclusively on automated processing.

4.1.4. Automated Decision-making

Just like with profiling, automated decision-making[122] and decisions made utilizing algorithmic means represent a potential threat to the data subjects' fundamental rights (Velasco and Viollier 2016).

According to Boyd and Crawford (2011), there is a tendency to show data analysis results as facts and not interpretation, thus covering automated decision-making under a mantle of objectivity. However, the programming of an automated mechanism or algorithm requires a decision regarding which data will be used to make the decisions and the parameters to be optimized, all of which are human decisions subject to the programmers' biases (Malik 2019). This way, it is possible for an automated mechanism to reach discriminatory or arbitrary results based on objective information. However, the technical complexity of these mechanisms and the fact that these algorithms are often protected by trade secrets and other intellectual property figures may obscure how these decisions are made. This explains comparative law's recent tendency to include tools to promote algorithmic transparency and the creation of rules that seek to protect people from this type of decision-making when it may have adverse legal effects on them.

Just like with profiling, the Chilean law has no figures explicitly created to address the issue of automated decision-making. The only relevant mention to automated data processing is in Article 2(o) of Law N° 19.628. When defining personal data processing, this article clarifies that the processing may or may not be automated.

---

122. For these effects, automated decision-making can be defined as "the ability to make decisions by technological means without human involvement" (Article 29 Working Party [2017] quoted in Newman and Ángel [2019, p. 56]).

For its part, the bill being discussed, employing the indications introduced by the Executive Branch, establishes the right to object to automated personal assessments, establishing in Article 8 that "[t]he data subject has the right to object to decisions concerning him or her taken by the controller, based solely on automated processing of his or her personal data, including profiling," with some exceptions.

This wording is also strongly inspired by Article 22 of the GDPR, which provides that "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Finally, although it is contained in the recitals, Recital 71 provides that the data subject has the right to "obtain an explanation of the decision reached after such assessment and to challenge the decision."

The wording of the article is nearly identical. A significant difference is that the GDPR allows for challenging the decision, whereas the regulation proposed in the Chilean bill only allows for requesting the decision to be reviewed. On the other hand, the Chilean bill does not require that, as part of the right to object, the automated decision should have legal effects on or significantly affect the data subject.

At least two of the companies studied make automated decisions based on the data collected from users. Facebook uses the information collected from the user's behaviour to provide personalized services. This way, Facebook makes decisions on the type of content to prioritize or show on the user's timeline. Similarly, this information is used by advertisers to provide directed advertisements. In both cases, the decisions made may be arbitrary or discriminatory. For example, Facebook was fined in the United States because its advertisers used user profiling to make advertisements based on discriminatory criteria, such as race, age, nationality, or disability (National Fair Housing Alliance 2020). Similarly, using automated decision-making for recruitment processes involves the risk of replicating selection biases based on criteria such as gender, as has happened in similar experiences (see Dastin 2018).

An interesting discussion on the topic emerged during the focus group. The participants emphasized the lack of transparency to make these decisions. An academic pointed out that:

> Many public entities use algorithms nowadays, but users cannot know what decisions are made or under what conditions or pa-

> rameters are these decisions being made. For example, when a bank rejects my loan application and they do not give any explanation. There is a difference between tools that make decisions and decisions made directly.

Similarly, a member of the civil society said that "the problem is that the algorithm is protected by intellectual property, and that hinders enforcement efforts."

4.2. What is Inadequately Regulated

4.2.1. Exceptions to the Principle of Consent

To protect individuals and ensure they maintain control over their data, the law provides—as a general rule—that third parties other than the data subject may not process personal data unless the subject consents. For this consent to be valid, according to Article 4 of Law N° 19.628, the data subject must be informed on the purpose of the data processing, and their eventual publication and authorization must be express and in writing. Similarly, the subject may revoke consent at any time, albeit not retroactively.

One of the main shortcomings of Law No. 19.628 is that it considers a series of exceptions to the subject's consent requirement. These exceptions are broad and undermine the law's capacity to protect. Jijena (2010) has asserted that these provisions mean that the lack of protection is the general rule, whereas the protection is the exception.

The most problematic exception is that contained paragraph (iv) of Article 4, which provides that:

> Processing personal data from or collected from publicly available sources do not require authorization when said data is of economic, financial, banking or commercial nature, is contained in lists relating to a category of persons which merely indicate background information such as the individual's membership to that group, profession or activity, educational qualifications, address or date of birth, or is necessary for direct response commercial communications or direct marketing or the sale of goods or services.

This exception implies that the data obtained from publicly available sources may be processed without the subject's consent and that the database controller will not have the obligation of respecting the purpose for which the data was collected or of maintaining the reserve on it, seriously

affecting the exercise of the rights to access, rectification, cancellation, and opposition (Alvarado 2014).

The jurisprudence has made an excessively broad interpretation of this exception, providing that any information available on the Internet or accessed by making a payment is a publicly available source. Thus, in the Ruling for Case N° 5.243 of 2015, the Supreme Court of Chile confirmed that the site 24x7datos, where an individual could find out the name of a person by entering their National ID Number, or vice versa, was legal as the information was on a publicly available source.

Section 6 of said article contains another exception and provides that:

> The processing of personal data by private legal persons for their exclusive use, by its associates and by its affiliates for statistical or fee purposes, or other general purposes that benefit them will not require said authorization.

Finally, Article 20 provides that "Personal data processing by a public entity may only be performed on the matters of its competence and subject to the above rules. The consent of the subject will not be required under these conditions." However, there is no adequate level of accuracy on whether the competencies should be expressly established regarding data processing or if it is a generic and relatively broad authorization. This has led public entities to interpret that they are always authorized to process personal data—even sensitive data—to the extent that said processing is on a matter related to their competences.

The bill does not seem to address these shortcomings. The project did not seize the opportunity to limit the sources that are considered publicly available to a closed list of cases. Instead, just like the current law, the draft opts for a broad definition of this category, understood as "all those databases or sets of public or private personal data, to which access or consultation may be lawfully made by any person, provided that there are no legal restrictions or impediments to access or use." However, the articles proposed to demand the consultation be performed lawfully, and Article 13(a) provides that, to make legitimate use of this exception, "Processing must be related to the purposes for which data were provided or collected."

There is also a slight improvement regarding processing by public entities. Article 20 of the bill provides that "the processing of personal

data by public entities is legal when performed to comply with their legal duties and within the scope of their duties." The mention of the compliance with legal functions within the scope of their duties presents interpretative elements to argue that such authorization must be among the attributions that the law expressly confers to the relevant public entity and that this authorization cannot be indirectly inferred through generic competencies of the public administration.

Finally, the bill's most relevant exceptions include the fact that it includes an exception not contained in Law N.° 19.628. Article 13(e) of the bill provides that the subject's consent will not be required "[w]henever the processing is necessary to meet legitimate interests of the controller or a third party, provided this does not affect the rights and freedoms of the subject."

Although the GDPR also considers the legitimate interest exception. Recital (47) mentions a series of elements that allow a more precise interpretation and provide more legal certainty to this concept. This way, it provides that:

> The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. […] At any rate, a legitimate interest would need careful assessment, including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place […].

Similarly, Article 6 of the GDPR does not contain a broad exception of the principle of consent because the information was obtained from a publicly available source. Regarding the processing by public authorities, Article 6 provides more restrictive criteria, demanding that the processing is necessary for the performance of a task carried out in the public interest vested in the controller.

The European regulation contains much more limited exceptions to the principle of legitimate interest, granting a higher standard of protection than the current Chilean law and the personal data protection bill.

The need for the subject's consent and the exceptions also sparked an interesting discussion in the focus group. A lawyer specializing in the field noted that "the strength of consent is diminishing; written consent is a bit anachronistic." The law focuses heavily on consent, and other legitimate interests lose relevance. Similarly, a civil society representative added that "responsibility is placed on the subject, which is detrimental to him or her."

4.3. The Law's Territorial Scope of Application

In Chile, the general rule is the application of the law's territorial principle. The exceptions to this principle are contained in Article 6 of the Organic Code of Courts. They include the prosecution of felonies such as piracy, those committed by a diplomatic agent in the exercise of his or her duties, those that threaten the sovereignty or the international security of the State, among others. This list does not contain any provision related to the protection of personal data. The same applies to the regulation of civil legal situations contained in the Civil Code.

Similarly, Law N° 19.628 contains no provision on the possibility of applying its extraterritorial provisions. Therefore, it is necessary to understand that the provisions of Law N° 19.628 can only be enforced concerning the processing of personal data that takes place within the territory of the Republic and that the rulings on the matter can only be made effective concerning data controllers domiciled in Chile.

Although the original bill did not contain any provision on its extraterritorial application, a final paragraph regulating the duties of database controllers was included in Article 14 during the legislative process. This way, it provides that:

> In addition to the obligations established above, the data controller not domiciled in Chile and processing the data of individuals residing within the national territory shall create and maintain an email address up to date and operational to receive communications of the data subjects and the Personal Data Protection Agency.

Whether this obligation will allow applying the decisions of a future personal data control public authority or the Chilean courts beyond national borders is debatable. However, it is a first step to, at least, prevent CDDBMs operating in Chile from being entirely disconnected from Chilean laws.

The GDPR presents a different perspective. Article 3 provides that "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." This way, the provisions of the GDPR apply to the processing of personal data of subjects residing in the Union by a controller or a processor not constituted in the Union when the processing activities are related to a) the offer of goods or services to the subjects in the Union, regardless of whether or not a payment is required, or b) to the monitoring of their behaviour as far as their behaviour takes place within the Union. The European Union has explicitly proposed the extraterritorial application of its data protection regulations. This way, their capacity to enforce their regulations and hold CDDBMs accountable is an improved situation concerning the Chilean law.

Europe may be able to enforce its legislation beyond its borders due to the size and influence of its market, which gives it real bargaining power with GAFAM. Consequently, the GDPR has had an expansive effect since its effective date. Many companies in the digital ecosystem have decided to make compliance with its provisions their global standard regardless of the jurisdiction of their users.

This analysis is particularly relevant in the case of Facebook, as it is the only one of the four companies studied that is not legally domiciled in Chile. This way, even if the personal data law bill is passed, a significant challenge regarding the application of the Chilean personal data protection regulations by Facebook will remain because its processing is subject to the jurisdiction of other countries. During the focus group, a representative of the industry pointed out that:

> It is incredibly complicated and is an issue common to all areas of law. If the offender has no assets in the country, you need to conduct the process abroad. You won't change that even if Facebook has a representative in Chile to serve. Being served a process is different from having assets to seize.

Similarly, an academic participating in the discussion noted that this problem is not exclusive to the protection of personal data and other areas of law. He said: "We are not having this debate in consumer law and other areas of law. Perhaps it should be addressed at the general level of private international law."

5. Evaluating the Capacities of the Data Protection Authorities

Chile has no controlling administrative authority for the protection of personal data. This implies that those individuals whose rights are violated must resort to the ordinary courts of justice. This procedural route involves a high entry barrier for most individuals, because of the economic costs, the requirement of attorney sponsorship, and how long such litigation typically takes. These factors have resulted in a small number of cases brought to the courts under Law N° 19.628, resulting in insufficient relevant case law on the subject. Similarly, the subjects have been deprived of an accessible, expeditious, and efficient mechanism to realize the rights granted by Law N° 19.628.

Another aspect that has hindered the application of Law N.° 19.628 is the low cost of the fines it establishes. For the database controller to be sanctioned for breaching any of the personal data law provisions, the subject must file a claim known as habeas data. This remedy applies in cases where the controller of the data bank fails to respond to a request of modification, cancellation, or suspension within two business days, or when the request is rejected.

This procedure is short and summary. If the claim is accepted, the ruling may impose a fine of 10 monthly tax reference units (approx. USD $686), or 10 to 50 monthly tax reference units (between USD $686 and USD $10,299) if the data is related to economic, financial, banking, or commercial obligations. Consequently, the cost of the fines is not significant enough to dissuade CDDBMs like GAFAM or a consolidated company that may easily consolidate the fines as operating costs.

In 2016, the Law Evaluation Committee published a report on the deficiencies of the Chilean personal data protection regulation. The methodology of the report included a series of interviews with experts on the subject. When asked about the adequacy of the judicial control mechanism contained in the current legislation, one of them expressed that "The current law clearly has problems, as it lacks effective enforcement mechanisms. Today, the transactional costs of claiming the breach of the right are so high that people simply do not claim it" (53).

Finally, note that Law N° 20.285 vested the Transparency Council with the power to ensure the correct compliance with Law No. 19.628 by the State Administration entities. However, there is no certainty of the scope of the governing verb "to ensure," and the vesting of this power was

not accompanied by any capacity to sanction non-compliance with the Council's decisions. For the same reason, this body has so far limited itself to officiating, requesting information, and issuing recommendations to other public bodies regarding the processing of personal data. However, it is impossible to assert that it constitutes a real control instance for public bodies.

This critical shortcoming of the Chilean Law seriously affects the law's capacity to hold the four CDDBMs studied accountable.

One of the main objectives of the bill being discussed in the Chilean Senate is to correct this shortcoming. The original bill considered the creation of a Personal Data Protection Agency, with functional autonomy but attached to the Ministry of Finance. Then, through a substitution indication in July 2018, the government of Sebastián Piñera chose to assign the Transparency Council the task of becoming the new Data Protection Agency, changing its name to the Transparency and Data Protection Council. Although it seemed ideal for the new entity to follow a model similar to the Spanish Data Protection Agency, that is, an autonomous, technical body with its own assets and independent from political powers. Subsequent governments ruled out this option arguing budgetary reasons.

Thus, the Senate had to decide between the Transparency Council and a new authority attached to the Ministry of Finance. Both models had pros and cons. The agency attached to the Ministry of Finance had a more technical specialty. It was a body exclusively devoted to the protection of personal data, but with reduced independence, as it directly depended on the ministry. On the other hand, the Transparency Council has significant autonomy, but it would not be a specialized body. Although the protection of personal data and access to public information are not necessarily mutually exclusive, they respond to an emphasis on particular legal assets, subject to the biases and training priorities of the professionals devoted to each area. On August 5, 2019, the Senate Constitution Commission—in a split vote—decided that the Transparency Council would become the new Personal Data Protection Agency (Biobío 2019).

Article 31 defines the powers vested in the Personal Data Protection Agency. The most relevant include:

> a) Officially apply and interpret the legal and regulatory provisions to be enforced by the Agency, and give general instructions to the legal or natural persons processing personal data.

> The general instructions given shall be issued following a prior public consultation through its official website.
>
> b) Monitor and ensure compliance with the principles, rights, and obligations outlined in this law. For monitoring effects, it may request any document, book, or record, as required.
>
> c) Resolve the queries and requests presented by data subjects against data controllers.
>
> d) Investigate and determine the infringements incurred by data controllers and exercise its sanctioning power according to the law [...].
>
> h) Develop outreach, education, promotion, and information programs, projects and actions aimed at the citizenry and the data controllers on the respect and protection of the right to privacy and the protection of personal data.
>
> [...]
>
> ñ) Resolve queries and requests regarding whether a particular database or data set is considered publicly available and identify the generic categories with such a condition.

This power to sanction is accompanied by increased fines and other sanctions to provide the law with effectively dissuasive tools when enforcing the provisions of the law. Thus, Article 39 of the law provides that:

> a) Minor infractions will be sanctioned with a written warning or a fine of 1 to 50 monthly tax reference units.
>
> b) Serious infractions will be sanctioned with a fine of 51 to 500 monthly tax reference units.
>
> c) Gross infractions will be sanctioned with a fine of 501 to 5000 monthly tax reference units.

Similarly, it provides the creation of ancillary fines in the event of repeated gross infractions, which consist of the suspension of the data processing operations and activities performed by the data controller for up to 30 days and the creation of a National Compliance and Sanctions Registry.

Conclusions and Recommendations

Following the description and analysis of the privacy policies and terms of use of Facebook, Falabella, PedidosYa, and AIRA, and considering the national regulatory and legislative landscape, we conclude that, following the global trend, CDDBMs in Chile consider data as a strategic asset regardless of their consolidation in the market. As such, the primary purpose of the data processing performed by these businesses is to attract new users and create new products at a minimum cost.

As shown above, the success of a CDDBM is proportional to its capacity to compile data and, especially, to interpret the information derived or inferred from such data. As a result, the close relationship between Big Data and AI will continue increasing and evolving, as macrodata may be used to train artificial intelligence systems such as neural networks and statistical models to predict events and behaviours. This information is considered highly valuable by these companies, as it allows them to understand and predict the market's current flow.

As mentioned in their respective policies, the primary source of data of CDDBMs is information directly collected from their users, from third parties (mobile-app developers, strategic partners, etc.), and by monitoring users with cookies. Regarding the data directly collected from users, there are still companies that require information on the user's gender as a condition to access the services (Facebook). On the other hand, concerning information obtained from third parties, the companies do not provide information on how they monitor and conclude that the data was lawfully obtained.

Web tracking through cookies has created new sources to collect data and, therefore, new processing purposes which go beyond providing the user with access to the service. Moreover, the most valuable and desired data processing by CDDBMs is performed with the primary purpose of profiling users and studying their browsing behaviour. On the latter, companies are not transparent about how their algorithms operate or the analytical tools they use to collect and process data.

These considerations raise many concerns about the unsatisfactory regulation and monitoring of CDDBMs at the national level. On the one hand, this is due to the obsolete data protection regulation, in force since 1999, and on the other, to the lack of an independent and specialized control body responsible for applying the current regulations.

In this context. We make the following recommendations:

CDDBMs should make their relationship with GAFAM more transparent. In the cases in which the company offers the possibility of signing up via a Facebook (PedidosYa) or Google (AIRA) account, the consequences of these actions for the processing of personal data should be explained. In this context, both the state and the civil society must promote communications campaigns aimed at educating the citizenry on the scope and main effects of accepting the policies and terms of use.

On the purpose of processing data, CDDBMs must clearly describe the purpose of each type of data processing. Likewise, they should not limit themselves to making a general reference to the use of cookies on the website. However, we also suggest they inform users about the type of cookies they use (persistent, analytical, personalization, etc.), the individualization of the data collection and analysis tools they use (a practice adopted by PedidosYa), and provide tools for objecting to this processing without losing access to the service.

The jurisprudential development of the concepts "privacy," "personal data," "sensitive data," "data controller," "publicly available source," and others, should be promoted. The above is considered necessary because the judiciary has rarely been able to reason and construct criteria in accordance with current times. This is partly due to the difficulty and lack of expertise to determine the legal right protected in technological environments, and partly due to the inefficacy of the habeas data provided under Law N° 19.628 of 1999, as it is a solely judicialized, long, and expensive procedure.

Establish a legal and institutional framework with sufficient capacities and powers to monitor the activities of GAFAM companies and establish dissuasive fines that cannot be attributed to the companies' operating costs.

References

Accenture Technology Vision. 2019. "The Post-Digital Era is Upon Us: Are You Ready for What's Next?" https://www.accenture.com/_acnmedia/pdf-97/accenture-technology-vision-2019-executive-final-brochure.pdf

Alvarado, F. 2014. "Las fuentes de acceso público a datos personales." *Revista Chilena de Derecho y Tecnología 3,* no. 2: 205–226. DOI:10.5354/0719-2584.2014.33276

APEC. 2009. "Cooperation arrangement for cross-border privacy enforcement." http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf

APEC. 2005. "Privacy Framework, APEC Secretariat." http://www.apec.org/Groups/Committeeon-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Becker, Sebastián, and Romina Garrido. 2017. "La biometría en Chile y sus riesgos." *Revista Chilena de Derecho y Tecnología 6*, no. 1. DOI:10.5354/0719-2584.2017.45825

Biobío. 2019. "Comisión de Constitución del Senado aprueba que cplt proteja los datos personales." https://www.biobiochile.cl/noticias/nacional/chile/2019/08/05/comision-de-constitucion-del-senado-aprueba-que-cplt-proteja-los-datos-personales.shtml

Boyd, Danah, and Kate Crawford. 2011. "Six Provocations for Big Data: A Decade in Internet Time." Symposium on the Dynamics of the Internet and Society. *ssrn Electronic Journal 123*, no. 1. DOI:10.2139/ssrn.1926431

Büchi, Moritz, Eduard Fosch, Christoph Lutz, Aurelia Tamò-Larrieux, Shruthi Velidi, and Salome Viljoen. 2019. "Chilling Effects of Profiling Activities: Mapping the Issues." SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379275

Canales, María Paz, and Pablo Viollier. 2018. "La compatibilidad de la retención general de metadatos y el respeto a los derechos fundamentales: el caso del decreto espía." In *Anuario de Derecho Público de la Universidad Diego Portales*, edited by R. Figueroa, 155–171. Santiago, Chile: Universidad Diego Portales. http://derecho.udp.cl/wp-content/uploads/2019/01/AnuarioDerPub_2018_INTERIOR_ok.pdf

Canales, María Paz. 2019. "¿Quién defiende tus datos? La problemática acción de Subtel." *Derechos Digitales*. https://www.derechosdigitales.org/13302/la-problematica-accion-de-subtel/

Cerda, Alberto. 2012. *Legislación sobre protección de las personas frente al tratamiento de datos personales : Material de estudio del Centro de Estudios en Derecho Informático*. Santiago, Chile: Universidad de Chile.

Chile, Chamber of Deputies. 2018. "Proyecto de Ley que Moderniza la legislación tributaria," August 23, 2018. https://www.camara.cl/pley/pley_detalle.aspx?prmID=12561&prmBOLETIN=12043-05

CIPER. 2019. "El empleado de Enrique Correa que opera como asesor de los senadores." *CIPER*. https://ciperchile.cl/2019/05/06/el-

empleado-de-enrique-correa-que-opera-como-asesor-de-los-senadores/

CNC. 2019. "Ventas de comida rápida crecieron un 5.4% durante el primer trimestre 2019." Cámara Nacional de Comercio, Servicios y Turismo. https://www.cnc.cl/ventas-de-comida-rapida-crecieron-un-54-durante-el-primer-trimestre-2019/

Comité Evaluación de la Ley. 2015. "Evaluación de la ley 19.628 Protección de la Vida Privada." http://www.evaluaciondelaley.cl/foro_ciudadano/site/artic/20151228/asocfile/20151228124429/informe_final_ley_19628_con_portada.pdf

Contreras, Pablo. 2019. "Propiedad de datos personales." *Apuntes de derechos*. https://www.pcontreras.net/blog/propiedad-de-datos-personales

Dastin, Jeffrey. 2018. "Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women." Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

Diaz, David, and Mohamed Zaki. 2015. *Innovación en Modelos de Negocios Basados en Datos*. Santiago, Chile.

DW. 2019. "EE.UU. multa a Facebook con US$5.000 millones por violación de privacidad." *El Mostrador*. https://www.elmostrador.cl/dia/2019/07/24/eeuu-multa-a-facebook-con-5-000-millones-por-violacion-de-privacidad/

Feldman, B. L., R. Adolphs, S. Marsella, A. Martinez, and S. Pollak. 2019. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements." *Psychological Science in the Public Interest 20,* no. 1. DOI:10.1177/1529100619832930

Hartmann, Philipp Max, Mohamed Zaki, Niels Feldmann, and Andy Neely. 2014. "Big Data for Big Business? A Taxonomy of Data-driven Business Models used by Start-up Firms" Cambridge Service Alliance, University of Cambridge. https://cambridgeservicealliance.eng.cam.ac.uk/resources/Downloads/Monthly%20Papers/2014_March_DataDrivenBusinessModels.pdf

International Data Corporation. 2018. "Predicciones de la industria TI para el 2018 en Chile." https://innovacionchilena.cl/wp-content/uploads/2018/03/PPT-Predicciones-CL-2018.pptx-1.pdf

Jijena, Renato. 2001. "Sobre la no protección de la intimidad en Chile : Análisis de la Ley 19.628 de agosto de 1999." *Revista electrónica de derecho*

e informática 39. https://libros-revistas-derecho.vlex.es/vid/intimidad-chile-analisis-19-628-1999-115523

Jijena, Renato. 2010. "Actualidad de la protección de datos personales en América Latina : El caso de Chile." En Memoria del XIV Congreso Iberoamericano de Derecho e Informática, Monterrey. http://biblio.juridicas.unam.mx/libros/6/2940/27.pdf

Malik, Momim. 2019. "Can Algorithms Themselves Be Biased?" *Berkman Klein Center*. https://medium.com/berkman-klein-center/can-algorithms-themselves-be-biased-cffecbf2302c

Montes, Carlos. 2018. "Diez años de Facebook en Chile." *Diario La Tercera*. https://www.latercera.com/tendencias/noticia/diez-anos-facebook-chile/106698/

National Fair Housing Alliance. 2020. "Facebook Settlement." https://nationalfairhousing.org/facebook-settlement/

Nava, Diana. 2018. "Aira, la robot que te reclutará para tu nuevo trabajo." *El Financiero*. https://www.elfinanciero.com.mx/tech/aira-la-robot-que-te-reclutara-para-tu-nuevo-trabajo

Newman-Pont, Vivian, and María Paula Ángel Arango. 2019. *Accountability of Google and Other Businesses in Colombia: Data Protection in the Digital Age.* Bogotá, Colombia: Dejusticia. https://www.dejusticia.org/publication/rendicion-de-cuentas-de-google-y-otros-negocios-en-colombia-la-proteccion-de-datos-digitales-en-la-era-digital/

OECD. 2002. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." Paris: Organisation for Economic Co-operation and Development. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface

Personal Data Protection Agency. 2017. Bulletin Nº 11.144-07. Law to regulate the protection and treatment of personal data and create the Personal Data Protection Agency [Chamber of Deputies, March 15, 2017; final revision, August 7, 2019]. https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07

Saldaña, María. 2001. "El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego." *Revista Teoría y realidad constitucional 28*: 279–312.

TrendTic. 2019. "Accenture Report: Adoption of Artificial Intelligence in Chilean Companies is More Advanced Than Global Companies." 15 April, 2019. https://www.trendtic.cl/2019/04/reporte-de-accenture-

adopcion-de-inteligencia-artificial-en-empresas-chilenas-estamas-avanzada-que-las-companias-globales/

Vega, Mayra, and Deysy Ramírez. 2018. "Start-up en las redes sociales." *Revista Espacios*. https://www.revistaespacios.com/a18v39n27/18392709.html

Velasco, Patricio, and Pablo Viollier. 2016. "Información financiera y discriminación laboral en Chile: un caso de estudio sobre Big Data." Santiago, Chile: Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/big-data-informe.pdf

Viollier, Pablo. 2017. "El estado de la protección de datos personales en Chile." Santiago, Chile: Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

We are Social and Hootsuite. 2019. "Essential Insights into How People Around the World Use the Internet, Mobile, Devices, Social Media, and E-Commerce." *Global Digital Overview*. https://www.slideshare.net/DataReportal/digital-2019-global-digital-overview-january-2019-v01

ACCOUNTABILITY OF COMPANIES WITH DATA-DRIVEN BUSINESS MODELS IN COLOMBIA: PERSONAL DATA PROTECTION IN THE DIGITAL AGE

María Paula Ángel-Arango
Vivian Newman-Pont
Daniel Ospina-Celis

1. Introduction and Selection of CDDBMs

In a previous study titled *Accountability of Google and other Businesses in Colombia: Data Protection in the Digital Age*, we analyzed the privacy policy of the products offered by thirty companies with a data-driven business model (CDDBM) operating in Colombia. To analyze them, we classified the companies into four categories: 1) large Internet companies, 2) intermediate companies, 3) start-ups, and 4) established companies. The first group comprises Google,[123] Amazon,[124] Facebook,[125] Apple,[126] and Microsoft[127] (usually known with the acronym GAFAM); all of these companies have a large innovation capacity and extensive capital to invest. The intermediate companies include those that, without being large Internet companies, cannot be considered start-ups either. These

123. Google LLC, "Google Privacy Policy" (no date). Retrieved June 1, 2018, from https://policies.google.com/privacy?hl=es-US&gl=us

124. Amazon Inc., "Privacy Notice" (no date). Retrieved June 1, 2018, from https://www.amazon.com/gp/help/customer/display.html?language=es_US&nodeId=468496

125. Facebook, "Data Policy" (no date). Retrieved July 25, 2019, from https://www.facebook.com/about/privacy/update

126. Apple Inc., "Privacy Policy" (no date). Retrieved June 1, 2018, from https://www.apple.com/legal/privacy/en-ww/

127. Microsoft Privacy Statement (no date). Retrieved June 1, 2018, from https://privacy.microsoft.com/en-us/privacystatement

include Netflix, Deezer, Spotify, Waze, or Uber. The third category, start-ups, applies to young companies with scalability and exponential growth (Entrepreneur 2019). These companies are usually national or regional at best. In the case of Colombia, companies like Rappi,[128] Cívico,[129] or Fluvip[130] were considered as start-ups. Lastly, the established companies include Almacenes Éxito,[131] Unilever,[132] Grupo Aval,[133] Sura,[134] and Claro,[135] which existed before the digital age but adapted to new technologies or created new data-driven business models.

The criteria to select the intermediate companies was their position in the *ranking* published by App Annie,[136] which analyzes the most downloaded App Store and Google Play applications in Colombia. The applications included in the top 10 most downloaded applications in Colombia during the first five days of July, August, and September 2018, respectively, were: WhatsApp, Tinder, Messenger, Facebook, Instagram, Facebook Lite, Netflix, Deezer, Google Drive, YouTube, LinkedIn, Messenger Lite, AliExpress, Joom, 30 Days Fitness Challenge, and 8fit Workouts and Meal

---

128. Rappi S.A.S., "Aviso de Privacidad" (no date). Retrieved June 1, 2018, from https://legal.rappi.com/colombia/politica-de-proteccion-y-tratamiento-de-datos-personales-rappi-s-a-s/

129. Cívico Digital S.A.S., "Políticas de Tratamiento de Datos Personales" (no date). Retrieved June 1, 2018, from https://www.civico.com/politicas-de-privacidad

130. Fluvip S.A.S., "Política para la protección y el tratamiento de datos personales de Fluvip" (no date). Retrieved June 1, 2018, from https://www.fluvip.com/home_policy_for_the_protection?locale=es_CO

131. "Política manejo de información y datos personales de Almacenes Éxito S. A." (no date). Retrieved July 1, 2018, from https://www.grupoexito.com.co/es/politica-manejo-de-informacion-y-datos-personales.pdf

132. Unilever N.V., "Privacy Notice" (no date). Retrieved June 1, 2018, from https://www.unilevernotices.com/united-kingdom/english/privacy-notice/notice.html

133. Grupo Aval Acciones and Valores S.A., "Política de privacidad y tratamiento de datos personales" (no date). Retrieved June 1, 2018, from https://www.grupoaval.com/wps/wcm/connect/grupo-aval/2c470a75-992f-4db3-a47b-a70da487464b/Politica-Tratamiento-Datos-Personales.pdf?MOD=AJPERES

134. Seguros Generales Suramericana S.A., "Política de privacidad y tratamiento de datos personales" (no date). Retrieved June 1, 2018, from https://www.segurossura.com.co/Paginas/legal/politica-privacidad-datos.aspx

135. Telmex Colombia S.A., "Política de tratamiento de la Información" (no date). Retrieved June 1, 2018, from https://www.claro.com.co/portal/recursos/co/legal-regulatorio/pdf/Politicas_Seguridad_Inf_Claro.pdf

136. App Annie, Top App Matrix, 2018. https://www.appannie.com/en/

Planner.[137] Although most of the applications mentioned above belong to a GAFAM company, seven of them are not owned by these companies. Therefore, their owner was considered an "intermediate company." Specifically, we studied the following intermediate companies: Match Group, LLC (Tinder)[138]; Netflix International B.V. (Netflix)[139]; Deezer S. A. (Deezer)[140]; Alibaba Group (AliExpress)[141]; SIA Joom Latvia (Joom)[142]; Bending Spoons S.p.A. (30 Days Fitness Challenge)[143]; and Urbanite Inc. (8fit Workouts and Meal Planner).[144] It must be said that this group of companies was completed with the following four companies whose applications, although not included in the top downloads ranking in Colombia during the first five days in any of these months, were top-rated in the country at the time of the study: Easy Taxi Colombia S.A.S. (EasyTaxi),[145] Spotify AB (Spotify),[146] Uber B.V. (Uber),[147] and Waze Mobile Limited (Waze).[148] Hence, the intermediate companies category included 11 companies.

Meanwhile, the criteria used in the study to select the sample of start-ups to analyze was their "affiliation to either Team Start-up Colombia or INNpulsa Colombia, the dynamic start-ups Colombian government agency" (Newman and Ángel 2019, 21). Considering the large number of

---

137. For a table compiling this information, see Newman and Ángel (2019, 22).

138. Match Group, LLC, "Our Commitment to You" (no date). Retrieved June 1, 2018, from https://policies.tinder.com/privacy/intl/en/

139. Netflix International B.V., "Privacy Statement" (no date). Retrieved June 1, 2018, from https://help.netflix.com/legal/privacy

140. Deezer S. A., "Personal data and cookies" (no date). Retrieved June 1, 2018, from https://www.deezer.com/legal/personal-datas

141. Alibaba Group, "Privacy Policy" (no date). Retrieved June 1, 2018, from http://rule.alibaba.com/rule/detail/2034.htm

142. SIA Joom (Latvia), "Joom Privacy Policy" (no date). Retrieved June 1, 2018, from https://www.joom.com/es/privacy

143. Bending Spoons S.p.A., "Privacy Policy" (no date). Retrieved June 1, 2018, from https://bendingspoons.com/privacy.html

144. Urbanite Inc., "Privacy Policy" (no date). Retrieved June 1, 2018, from https://8fit.com/privacy/

145. Easy Taxi Colombia S.A.S., "Aviso de Privacidad" (no date). Retrieved June 1, 2018, from http://www.easytaxi.com/co/terms-conditions/aviso-de-privacidad/

146. Spotify AB, "Spotify Privacy Policy" (no date). Retrieved June 1, 2018, from https://www.spotify.com/us/legal/privacy-policy/

147. Uber B.V., "Privacy Policy" (no date). Retrieved June 1, 2018, from https://privacy.uber.com/policy

148. Waze Mobile Limited, "Privacy Policy" (no date). Retrieved June 1, 2018, from https://www.waze.com/es-419/legal/privacy

start-ups in the country, we did not include all the initiatives of both initiatives, but only those which still exist and for which their privacy policy was easily available. In addition to those selected this way, we included two companies which, even if not included in the portfolios, offer applications with noteworthy data processing models. Finally, we selected established companies from the largest companies in Colombia in the following sectors: mass market, retail, insurance, financial, and telecommunications. The sample of CDDBMs described above did not intend to be exhaustive, but merely illustrative of the type of companies currently collecting data in Colombia. The findings reported here correspond to the content of the Privacy Policies reviewed at the time of drafting the book *Accountability of Google and other Businesses in Colombia: Data Protection in the Digital Age*, which correspond to the dates of the "latest update" reported in Annex 1 of the book.

2. Operations of CDDBMs Collecting Data in Colombia

Upon reviewing the privacy policies of the products offered by the 30 CDDBMs studied, we found that there are specific patterns in their operations, which were grouped in the following categories: 1) data sources, 2) processing, 3) purpose of data processing, and 4) relationship with GAFAM.

2.1. Data Sources

Regarding the data sources, we found that most CDDBMs operating in Colombia have three primary sources of data. First, the user/customer usually provides their data when creating an account or profile, making a purchase, or uploading content to the platform or application. In some cases (e.g., Facebook and Tinder), the information provided may constitute sensitive data such as political views, ethnicity, sexual orientation, beliefs, interests, etc. In other cases, like Unilever, while the services or products requested may not directly imply the collection of special categories of data, these may suggest sensitive data, such as religious beliefs or the health status of the data subject.

The second source of information includes data collected through web tracking. This source includes data on the applications, devices, or browser used by the user/customer, and on the activity performed in the platform or application. Similarly, it includes data on the user's location,

even when the application is not in use. Some companies, such as Duety,[149] consider that the data collected through web tracking does not constitute personal information, as they are not linked to the user but to the Internet Protocol (IP) addresses and similar identifiers of the device used. Similarly, Apple mentions that it will only consider IP addresses and similar identifiers as personal data if the local laws consider them as personal data.

The third most common source of data is data provided by strategic partners. This type of data is not collected by the platform or the application, but comes from a third party, including 1) companies providing services on behalf of the company; 2) advertisement companies providing marketing or research services; 3) third-party platforms in which the company has an account; 4) third parties who process and analyze the personal data held by the CDDBM; 5) companies to which they provide services; and 6) credit bureaus used by the companies in their applications and platforms.

Although less used, the other data sources identified were the acquisition of information from external data providers, free-access data on the web, the use of sensors and devices, and crowdsourcing.

2.2. Processing

Regarding how personal data is processed, we found that the CDDBMs operating in Colombia are mainly involved in two activities: 1) collection, and 2) analysis. Data is usually collected by using various technological tools with technical specifications that allow collecting data. The most common tools used are a) proprietary or third-party cookies: files sent to a user's computer when he or she visits a website, allowing the site to recognize the computer upon revisiting the site; b) advertising identifiers: their function is very similar to cookies, but on a mobile device; c) pixel tags: they allow monitoring an activity (for example, when a site is visited or an email read); d) software development kits (SDK): cookies or pixel tags on apps; e) browser's web storage: the website stores data in a device's browser; f) application use caches: information saved on a device that allows a website to load faster or work without an Internet connection; g) server registries; h) tracking URL addresses: links that allow knowing the source of a website's traffic comes. Note that different types of cookies

149. Duety S.A.S., "Legal" (no date). Retrieved June 1, 2018, from https://blog.duety.co/legal/#privacidad

collect different types of information. CDDBMs use one or various types of cookies, depending on the data they intend to collect.

On the other hand, their analysis of the data is more uniform. Mainly, they perform a descriptive analysis aimed at segmenting and classifying users according to their tastes, preferences, or interests; or a prescriptive analysis to improve the user's experience in future visits. However, the applications' privacy policies contain no detailed technical information to determine the technological tools that each product uses to analyze data.

In contrast with the collection and analysis, the privacy policies of the CDDBMs operating in Colombia rarely recognize the sale or trade of data as a form of processing. Notably, the only company that openly recognizes this type of processing is Cívico. In contrast, some of the companies studied (e.g., Amazon, Facebook, and Uber) mention that they are not engaged in the business of selling their customers' data to third parties. However, this does not prevent the companies from pointing out that, should the company be acquired by a third party, the personal data of the users/customers will be one of the transferred assets.

2.3. Purposes

The analysis of the privacy policies of the sample of 30 CDDBMs showed nine primary purposes for processing personal data: 1) provide an excellent service; 2) communicate with the user; 3) develop new products or services; 4) manage sweepstakes, discounts, or other offers; 5) conduct market research; 6) offer personalized content (e.g., advertisement); 7) calculate the performance of the content; 8) conduct studies and research; 9) share information with third parties. There are two notable cases regarding the latter. First, 8fit Workouts and Meal Planner, whose privacy policy includes a list of all the applications that are linked to it, and the partners with whom it shares data. Second, WhatsApp, which when sharing information with third-party applications or Facebook, "requires them to use your information on our behalf in accordance with our instructions and terms."[150]

In addition to these common nine purposes, Cívico also includes the creation of a database that may be traded among its purposes. Similarly, Duety includes the assignment of the database among its purposes. Finally, Unilever's processing purposes include automated decision-making,

150. "WhatsApp Privacy Policy" (no date). Retrieved June 1, 2018, from https://www.whatsapp.com/legal?eea=0#privacy-policy

understood as making decisions exclusively through automated means, with no intervention by human beings.

2.4. Relationship with Google, Apple, Facebook, Amazon, and Microsoft (GAFAM)

As these are the largest Internet companies, most applications interact with some of the products offered by GAFAM. Thus, the CDDBMs studied relate with GAFAM, mainly in four ways: 1) the application or website allows signing in through a third party or social media site (Facebook, Gmail, etc.); 2) the app or website has social media buttons provided by Facebook, Google+, LinkedIn,[151] or Twitter; 3) the application or website uses Google Analytics (site's data service analysis); or 4) their advertisement partners include companies that are part of Google. On the one hand, these relationships allow CDDBMs to use the personal data provided by GAFAM, and on the other, allows GAFAM to access the information held by the CDDBMs.

3. How Prepared are the Colombian Personal Data Protection Regime and the Competent Authorities to Face the Challenges Posed by the Digital Age

Considering how the CDDBMs studied operate, we will now analyze the preparedness of the Colombian personal data protection legal regime and the competent authorities to protect personal data from the sources, purposes, and forms of processing of the digital age.

Data protection in Colombia is recognized under Article 15 of the Political Constitution and two statutory laws that develop the fundamental right to habeas data: Statutory Law 1266 of 2008,[152] on the right to the protection of financial, credit, commercial, and services information from third-party countries; and Statutory Law 1581 of 2012, on the processing of personal data in general. These laws contain basic data processing

---

151. "LinkedIn Privacy Policy" (no date). Retrieved June 1, 2018, from https://www.linkedin.com/legal/privacy-policy

152. Statutory Law 1266 of 2018, "Whereby the general habeas data provisions are issued and the management of information contained in personal databases, especially financial, credit, commercial and services information, and that coming from third-party countries is regulated and other provisions are issued." December 31, 2008. D.O. 47.219. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

principles, such as the principle of purpose, transparency, restricted circulation, security, and confidentiality. Furthermore, they create special legal categories, such as sensitive data and data on boys, girls, and teenagers.

Although groundbreaking at the time, these regulations fail to consider the issues of the digital age. Upon studying the behaviour of CDDBMs via computer platforms and a thorough reading of the law, we find that the legislation currently applicable in Colombia does not cover some phenomena identified when analyzing the operations of CDDBMs. These include: 1) inferred sensitive data, 2) IP-related data, 3) use of cookies, 4) web crawling, 5) data trading, 6) personalized content, and 7) automated decisions. However, there are other cases of data use which, even if considered in the law, their regulation is not in line with the digital age (for example, regarding the free and informed consent).

3.1. What Is Not, but Must Be, Regulated

The current regulations do not consider some situations of the digital age, which imply insufficient protection for data subjects.

Inferred sensitive data and data that leads to infer sensitive data pose a challenge for the national legislation considering the practices of CDDBMs. According to Article 5 of Law 1581 of 2012, sensitive data is data that "affects the intimacy of the Data Subject may cause discrimination if misused." These data do not necessarily have to be provided by the data subject, but may be inferred or acquired through data crossing. Hence, the processing of inferred sensitive data, just like that of sensitive data, is forbidden in Colombia, except in cases mentioned in the law (Article 6). Furthermore, the practices of CDDBMs show that non-sensitive data (for example, purchases from Amazon.com) may be used, along with other data, to infer sensitive personal data (e.g., a person's sexual orientation). The shortcoming of the Colombian law is that it does not consider that specific personal data may be used to obtain (infer) new information on the subject. Doctrinal and jurisprudential developments on the concept of sensitive data as established in Article 5 of Law 1581 of 2012 are urgent to clarify that it includes not only the data that may affect the privacy of an individual or lead to discrimination but also that which, although in principle does not imply a risk, allows inferring or deriving sensitive data of the subject when combined with other data.

Another issue not regulated under the current legislation is related to online identifiers, e.g., Internet Protocol (IP) addresses, which

allow relating it to an individual through their device's information. The Colombian law does not directly refer to this issue. It does not seem to imply that the IP addresses and other identifiers allow identifying a specific individual. However, Article 3(c) of Law 1581 of 2012 seems to consider online identifiers within the concept of personal data. It defines personal data as "any information related or that may be related to one or several determined or determinable natural persons." Considering that the European Union General Data Protection Regulation (GDPR) (Article 4), the California Consumer Privacy Act (CCPA) (Section 1798.140)[153] and the Article 29 Working Party recognize IP addresses as personal data, it does not seem inappropriate to interpret the Colombian legislation to include web identifiers within the category of personal data. In any case, the national law does not directly refer to this case, and therefore, allows companies not to recognize it adequately, as in the case of Apple, which does not consider the IP address as personal data if the legislation of the respective country does not do so.

According to the characterization of how the CDDBMs operate in Colombia, the use of cookies is one of the leading practices in the digital world and allows collecting massive amounts of information. Therefore, national legislation should respond accurately to the dynamics and risks of this technological tool. However, since the data protection authority considers that an adequate interpretation of the current data protection regulation is enough to protect the rights of Colombians, it has stated that "there is no specific regulation on the use of cookies in Colombia."[154] Therefore, at least to the letter, the current law treats personal data collection through cookies as any other type of personal data processing. This implies that there are no restrictions on the tool used for the collection, even less on the cookies that may be implemented. This means that the legal guarantees, obligations, and limitations applicable to data processing, including, for example, obtaining prior and informed consent from the data subject, also apply to the data collected through cookies. However, on the latter, note the case of the European Union, which not only has limitations and exceptions to the subject's consent—specifically

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

154. Superintendence of Industry and Trade, Opinion 14-218349-4-0, March 3, 2016.

regarding cookies—but the regulation is even more stringent regarding the consent for behavioural advertisement cookies.

In the light of this contrast, we believe that a further doctrine, jurisprudential or legal development on the use of cookies to collect personal data online in Colombia is critical, thus imposing more considerable limitations or safeguards to provide consent, except for cookies which 1) are essential for the service requested to function; or 2) collect anonymized or aggregated data.

Another phenomenon that appears to be unregulated is the marketing of personal data. Although, to a lesser extent, we also noticed it in some of the privacy policies of the products offered by the CDDBMs studied here. Data has an economic value, and this has made buying or selling it a usual practice in the digital age. However, the only reference to the marketing of personal data in Colombia is in Article 269F of the Criminal Code, not in the data protection laws. This code provides that:

> Who, *without being authorized to do so*, for their benefit or that of a third party, obtains, compiles, subtracts, offers, *sells*, exchanges, sends, *purchases*, intercepts, discloses, modifies or uses personal codes or personal data contained in archives, files, databases or similar means, shall be liable to imprisonment (emphasis added).[155]

From this article, we can conclude that the marketing of data in files, archives, or databases is, in principle, permitted, and that the prohibition on marketing only applies without authorization. However, when is someone authorized? Based on the principle of personal freedom, the subject's prior and informed consent could authorize the data controller to sell personal data.

However, this free power to sell could imply a risk of discrimination, massive surveillance, and civil freedoms restriction, especially considering the practices of data brokers who profile the data subjects. This situation contrasts with the CCPA, which allows consumers to forbid the sale of their personal information by a company (which the law defines as the right to opt out), and forbids the company from retaliating or discriminating against a consumer for exercising this right in terms of the price or

155. Law 599 of 2000, "Whereby the Criminal Code is issued." July 24, 2000, DO. 44,097. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

quality of the good or service they offer, with few exceptions. Additionally, companies are forbidden from selling the personal information of consumers under 16 years of age, unless the minor (in the case of children between 13 and 16 years of age) or their parents (for children between 0 and 13 years of age) authorize it (defined in the law as the right to opt-in). Similarly, the incipient Colombian regulation contrasts with the case of the European Union. Conscious of the potential that the sale of personal data creates for profiling, through the GDPR the European Union has attempted to promote transparency in profiling and encouraging the fair nature of data processing, including profiling.

Taking into account these contrasts, a greater doctrinal, jurisprudential, or legal development on the following is desirable: 1) the processing of data whose purpose is the commercialization of data, so it is subject to further safeguards than those offered by the principle of purpose, as provided in Article 4(b) of Law 1581 of 2012; and 2) profiling, to ensure—at least—the transparency and fair nature of the profiling process, preventing vague categorizations based on erroneous or discriminatory data.

Furthermore, unlike other legal regimes, the Colombian personal data protection law does not consider the right to data portability. Data portability implies that the data subject may "transfer" their data autonomously from one data repository to another. This includes the access to an electronic copy of all the data provided or subject to processing—to transfer them to a different company/controller—and that the data controller directly transfers them to another controller under the instructions of the data subject. Despite being recognized in some regulatory instruments such as the GDPR (Article 20) and the Ibero-American Standards (Article 30), the right to data portability still poses many questions. For instance, does the portability imply the transfer of all data or only those provided by the subject? Can a controller keep copies of the information on which portability rights have been exercised for transfer purposes? Both experts and the industry have given mixed answers to this and other questions. For example, according to the Ibero-American Standards, data portability does not apply to information derived or obtained from analysis (Article 30.4). For its part, in September 2019, Facebook published a document titled *Charting a Way Forward on Privacy and Data Portability*. Rather than setting out the company's position on the issue, it asks awkward questions on five aspects regarding data portability (Egan 2019).

Another matter with no specific regulation is the offer of personalized content (especially advertisement), which most of the CDDBMs studied mentioned as one of the purposes of their data processing. After reviewing Law 1581 of 2012, it is apparent that this purpose has no special regulation beyond the general obligations of the purposes for which personal data may be processed. Therefore, the only mention to this matter in the Colombian legal regime is that the purpose must be legitimate according to the Constitution and informed to the subject when collecting personal data. This insufficient regulation does not consider that content personalization is based on profiling, a practice that, we reiterate, may compromise every person's rights and freedoms. Furthermore, it disregards the fact that personalized advertisement is not always equal but can be more or less invasive, depending on whether it is contextual, targeted, or behavioural. The latter affects the right to privacy the most, as it is created based on people's behaviour on the Internet through time.

In light of these risks, we consider that a further doctrinal, jurisprudential, or legal development of data processing, whose purpose is the provision of personalized content (specifically when it comes to behavioural advertising), is critical in Colombia so that, just like data marketing, they are subject to higher safeguards than those offered by the principle of purpose.

Finally, automated decision-making is another phenomenon that, according to the review of privacy policies studied here, emerges as a result of the digital era and is not regulated by the Colombian data protection legislation. In this case, the current regulation fails to address several risks when it comes to collecting data to make automated decisions. This lack of specific regulation contrasts with the provisions of the Guiding Principles on Business and Human Rights and the United Nations Resolution on the Right to Privacy in the Digital Age A/C.3/71/L.39,[156] especially with the provisions of the GDPR which gave the data subject the option to oppose to automated processing if it produces legal effects or significantly and similarly affects them and, furthermore, it demanded the data controller to adhere to certain participation obligations of the data subject and human third parties.

156. United Nations General Assembly, Resolution A/C.3/71/L.39, "The Right to Privacy in the Digital Age." October 31, 2016. https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx

In the light of these developments, we believe that Colombia must have a further doctrinal, jurisprudential, or legal development on the processing of data for automated decision-making, so that it is subject to more significant safeguards than those offered by the principle of purpose.

3.2. What is Inadequately Regulated

The digital age and the use of mobile applications and technological platforms by CDDBMs have led to new phenomena that require the creation of a new law and have also changed the conditions under which the current regulations should be applied. This is the case of the possibility of sharing personal data for academic research and the prior, express, and informed consent.

First, the Colombian legal regime considers the possibility that the data controller shares data with third parties for academic research (notably, with historical, statistical, or scientific purposes). In this case, under Article 10(d) of Law 1581 of 2012, the authorization of data subjects shall not be necessary, and sensitive data could even be processed provided "measures aimed at suppressing the identity of the Data Subject are adopted" (Article 6(e), Law 1581 of 2012). However, given the volume of data processed nowadays, the requirement to anonymize sensitive data is insufficient because, even if this precaution is taken, the data subject can be re-identified if a considerable amount of personal data is available. In contrast, in cases like the European Union, the GDPR requires anonymization to be accompanied by a *compatibility assessment*.

Second, in Colombia, consent is considered as given upon accepting the platform or application's privacy policies. While available to all users, these policies are: 1) difficult to read, due to their length, 2) difficult to understand, due to their complexity, and 3) difficult to assess in practice, due to their ambiguity. Furthermore, these policies do not allow the subject to overcome previous obstacles, select the processing and purposes they wish to authorize, and opt-out of those with which they disagree. The information is presented en bloc and must be entirely accepted or rejected. In these circumstances, the usefulness of the prior, express, and informed consent to protect the rights of individuals and, specifically, the right to the protection of personal data in a big data environment, in which many of the purposes of data processing have yet to be defined, is doubtful. This contrasts with practices such as those in the European Union, which

allow, for example, "Separate consent to be given to different personal data processing operations" (Recital 43, GDPR).

Thus, it is time for a further doctrinal, jurisprudential, or legal development on the prior, express, and informed consent of the data subject in Colombia so that the unconditional consent for each specific purpose is required, as well as the express mention to it via a statement or explicit affirmative action, at least in the cases of processing of personal data for profiling, data marketing, the provision of behavioural advertising, or automated decision-making.

3.3. The Law's Scope of Application

According to Article 2 of Law 1581 of 2012, the regulation shall apply in two scenarios: 1) "to the processing of personal data performed in Colombian territory," and 2) "when the Colombian law applies to the data controller or processor not constituted in the national territory under international regulations or treaties." The text of this article indicates that the law does not apply to companies not domiciled in Colombia (such as all GAFAM companies and most "intermediate companies"), as most of their data processing activities are performed outside of Colombia. This was the initial consideration of the Deputy Superintendence for the Protection of Personal Data of the Superintendence of Industry and Trade. In 2014, when analyzing whether the Colombian data protection law applied to a company controlling a social media site, the Deputy Superintendence argued that the Colombian data protection law was not applicable because the "collection, use, storage or suppression of personal data is not performed in Colombian territory, as the social media sites are not domiciles in Colombia."

However, in 2016, the SIC changed its interpretation of the law's scope of application and provided that it applied in countless scenarios, including "the processing of personal data performed by the providers of social media services domiciled outside of Colombia, through 'means' located in Colombian territory."[157] In this sense, it is understood that when the data protection authority mentions "means," it refers to cookies, which are stored in the user's computer upon visiting a website. The computer, and hence the cookies, are located in Colombian territory.

157. Superintendence of Industry and Trade, Opinion 14-218349-4-0 dated March 3, 2016.

In this scenario, when publishing *Accountability of Google and other Businesses in Colombia: Data Protection in the Digital Age*, we mentioned that:

> we believe that although the second opinion of the Deputy Superintendence for the Protection of Personal Data provided the obligations and safeguards contained in Law 1581/2012 with a greater territorial scope, there is still much room for improvement. Consider the European Union where, based on the GDPR, the territorial scope of the European personal data protection regulations stopped depending on the location of the controller or processor, their establishments, or the means used to process the data. In contrast, it began to rely on the location of the personal data subjects being processed (Newman and Ángel 2019, 76–77).

Concurrently with this call, the Deputy Superintendence for the Protection of Personal Data of the Superintendence of Industry and Trade extended its interpretation of the law's scope of application. Thus, in Resolution 1321 of 2019, the Directorate of Investigations of the Deputy Superintendence for the Protection of Personal Data considered that Law 1581 of 2012 applies to foreign companies collecting data of Colombian citizens in the national territory.[158] In this resolution, which issues specific orders for Facebook to comply with the national regulations and ensure the security of information, the data protection authority stipulates that the regulation applies to the "processing of personal data performed in Colombian territory regardless of whether the Controller or Processor is physically located in the territory of the Republic of Colombia." Furthermore, it states that, although a good part of the processing of personal data is done on the Internet, "This does not mean that the obligation to comply with local standards and respect human rights disappears because of this technological phenomenon."

Following this interpretation, the Deputy Superintendence for the Protection of Personal Data issued another resolution further developing the argument on applying the law to companies not domiciled in

158. Superintendence of Industry and Trade, Resolution 1321, "Whereby orders are issued as part of an administrative process." January 24, 2019. https://www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf

Colombia. Resolution 21478 of 2019 orders Uber to ensure the safety of the data and comply with the national law. Regarding competence, it stated that:

> Statutory Law 1581 of 2012 applies to any operation on pieces of information related—or which may be related—to natural persons living or domiciled in the Republic of Colombia by, for example, mobile applications developers, even if their headquarters are not in Colombian territory and even when processed abroad.[159]

The interpretation of the scope of application of the data protection law combines three elements: the domicile of the data subject, just like GDPR; a broad understanding of the term "processing," which includes, by definition, the collection of data; and the fact that the collection takes place in Colombia. More specifically, the Deputy Superintendence for the Protection of Personal Data of the SIC provides that:

> A good part of the processing of personal data is made on the Internet, which facilitates, for example, the collection of information in Colombian territory and that said data is processed or used outside of Colombia. However, this does not mean that the obligation of organizations operating globally of complying with the local rules, effectively and completely ensuring the right to the protection of personal data and respect human rights disappear due to that technological phenomena.[160]

Additionally, the interpretation by the SIC adjusts to the Constitutional Court's criteria on the application of the law to transnational companies. For example, when analyzing the constitutionality of Article 2 of Law 1581 of 2012, the Court stated that said provision was in line with the Constitution, because it:

> Extends the scope of protection to the processing of personal data performed outside of the national territory, according to the subjective factor. In a globalized world where transborder data flows are constant, the extraterritorial application of the protection standards is fundamental to ensure adequate protection to the

159. Superintendence of Industry and Trade, Resolution 21478, "Whereby orders are issued as part of an administrative process." June 17, 2019. https://www.sic.gov.co/sites/default/files/files/Noticias/2019/ORDEN%20%20UBER.pdf

160. Ibid.

> rights of residents in Colombia, as many processing takes place precisely beyond its borders thanks to new technologies.[161]

This novel interpretation by the Deputy Superintendent is an improvement in the protection of Colombians' personal data in the digital age because, in line with the constitutional jurisprudence, it enables the data protection authority to hold CDDBMs not domiciled in Colombia accountable. However, it should not be overlooked that the two resolutions reviewed above (in the Facebook and Uber cases) are private administrative acts that have not been subjected to judicial review.

The Constitutional Court seems to support the rule of extraterritorial application of the right to personal data protection; however, when resolving other types of cases related with the moderation of content published on social media sites and other digital platforms (Twitter, Blogger, YouTube, etc.), where the Court developed the thesis of the lawfulness of judicial orders addressed to the administrators of the platform to ensure the adequate protection of the fundamental rights to privacy and reputation. Recently, in Ruling SU-420 of 2019, when resolving a case involving possible liability by Google LLC and Google Colombia for publishing an allegedly dishonourable message on a blog hosted on the Blogger.com platform—owned by Google—the Court considered in obiter that the intermediaries were "subsidiarily" liable when deleting the content directly through its editor was impossible. On this matter, the Court stated that:

> Although the sites use tools to facilitate electronic publications, they are not responsible for breaching people's rights to honour and reputation, as they have the possibility of removing the vexatious content disseminated on its portals and, therefore, as administrators of the platform, they are the only actors capable of stopping a rights violation by deleting the post that violates the fundamental rights of an individual. They may be included in the proceeding and be the subjects of an injunction seeking the termination of the act constituting the alleged transgression.[162]

---

161. Constitutional Court of Colombia, Ruling C-748 of 2011, (Judge writing for the court: Jorge Ignacio Pretelt: October 6, 2008). http://legal.legis.com.co/document/Index?obra=jurcol&document=jurcol_c5d6d39c403e0084e0430a0101510084

162. Constitutional Court of Colombia, Ruling SU-420/19 dated September 12, 2019. Judge writing for the court: José Fernando Reyes. https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm

3.4. Capacity of the Deputy Superintendence for the Protection of Personal Data of the Superintendence of Industry and Trade to Regulate, Sanction, Monitor, and Control

Unlike in other countries of the region (where there is no authority at all) or in the United States (where no authority is legally vested with monitoring powers, but the Federal Trade Commission assumed them de facto), Colombia has a data protection authority responsible for monitoring and ensuring that the processing of personal data respects the principles, guarantees, and procedures contained in Law 1581 of 2012. According to the Colombian law, the Deputy Superintendence for the Protection of Personal Data of the Superintendence of Industry has the following duties: 1) monitor and control duties to ensure the compliance with the data protection law and require the data controllers demonstrate that they have implemented measures to comply with their obligations under Law 1581 of 2012, and manage the National Databases Public Registry, and 2) disciplinary functions, which include conducting investigations and, as a result, order measures to enforce the right to habeas data and request the collaboration of international entities whenever the rights of data subjects beyond the Colombian territory are affected.

In practice, the Deputy Superintendence for the Protection of Personal Data has improved its disciplinary, monitoring, and control capacities throughout the years. For example, one of the most notable advances is the specialized personnel working for the Deputy Superintendence. In 2017, the entity had approximately 30 officers, whereas in 2020, it had 73 employees. This means that the entity doubled its workforce in three years, which allows it to better perform its duties.

The data available show a change in the Deputy Superintendence's monitoring and control capacities during the last four years. According to the statistics available on the performance of the SIC, in 2016, the Deputy Superintendence processed about 6,000 complaints on habeas data and issued almost 400 orders or fines. In 2019, the same Deputy Superintendence—now with twice as much staff—processed over 12,000 complaints on habeas data and issued almost 1,000 orders or fines. This means that the SIC doubled its sanctioning, monitoring, and control capacities on the protection of personal data in proportion to its workforce.

Recently, the Deputy Superintendence has focused part of its work on the processing of personal data in the digital age. Between 2018 and 2019, as part of the Ibero-American Data Protection Network, this

Deputy Superintendence led the creation of guidelines on 1) data processing and Artificial Intelligence, 2) data processing for e-commerce, 3) data processing for marketing and advertisement, 4) demonstrated liability in international transfers of personal data.[163] Although these guidelines are not binding regulatory instruments for personal data controllers, they constitute best practice standards that should be considered.

The increased working capacities of the Deputy Superintendence have resulted in the promulgation of several decisions on data protection in the digital age. Three of them are worth mentioning.

The first one is Resolution 74828 of 2019. In this case, the Deputy Superintendence decided to confirm the sanction imposed on Rappi, a courier services brokerage platform, for violating the principle of freedom. The Deputy Superintendence confirmed the difference between singing up and the authorization for the processing of personal data, and considered that:

> The creation of user profiles in the technological platform does not imply, per se, that [the subject] authorized the processing of his or her data. On the contrary, creating a user profile requires authorization from the subject when personal data are used for such effects.[164]

In this decision, the Deputy Superintendence sends a clear message to the CDDBMs to differentiate both processes and refrain from taking the fact of accepting the terms and conditions or clicking on the privacy notice as a formal authorization to process personal data.

The second relevant decision is Resolution 76538 of 2019. In this case, the company Asegúrate Fácil Ltda. informed its digital users that upon clicking on the "*calcular valour*" button on their website, they accepted the company's privacy policies and, therefore, authorized the processing of personal data. The Deputy Superintendence confirmed the sanction imposed and clearly stated that clicking a button with no relation to the processing of personal data was not appropriate to give valid

---

163. 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

164. Superintendence of Industry and Trade, Resolution 74828, "Whereby an appeal is resolved." December 17, 2019. https://www.sic.gov.co/sites/default/files/boletin-juridico/Res%2074828%20del%2017XII2019%20Rappi.pdf

consent. On this matter, the Deputy Superintendence informed that "silence, boxes 'pre-checked' and inaction do not constitute consent under Law 1581 of 2012."[165]

In third place, Resolution 54265 of 2019, where the Deputy Superintendence considered that using the web platform offered by Facebook Inc. to collect data does not release the controller from complying with Law 1581 of 2012 and its regulatory standards.[166] In this case, it decided to require the company Wikimujeres S.A.S. to respect the rights of the subjects of the data it collects through a linked domain in facebook.com.

3.5. Competence Regarding the CDDBMs

The Deputy Superintendence for the Protection of Personal Data of the Superintendence of Industry and Trade has competence over Colombian companies and foreign companies to whom the data protection law applies. However, in practice, the Deputy Superintendence has faced difficulties in asserting its authority over the controllers or processors not domiciled in Colombia. Despite the progress described in the section on the scope of application of Law 1581 of 2012, the decisions contained in the Resolutions on Facebook and Uber were appealed. According to Uber and Facebook, the Colombian data protection regulations do not apply to them because they are not domiciled in Colombian territory and because they process-analyze information outside of Colombia.

However, in Facebook's case, through Resolution 4885 of 2020, the Deputy Superintendence for the Protection of Personal Data resolved the remedy presented by the CDDBM on February 13, 2020. There, it confirmed the first-instance decision and reiterated that Facebook Colombia S.A.S. is a subsidiary of Facebook Inc.; that the business model of Facebook Colombia S.A.S. is based on the collection, use, and transmission of information by Facebook Inc.; that Facebook Colombia S.A.S. processes personal data, and; that the Colombian Constitution and Laws apply to the processing. This decision sets out the final position of the national personal data authority. In any case, despite the importance of the resolution on Facebook's case, the capacity of this authority to hold the CDDBMs not domiciled in Colombia accountable for the processing of

165. Superintendence of Industry and Trade, Resolution 76538, December 27, 2019.

166. Superintendence of Industry and Trade, Resolution 54265, October 11, 2019.

personal data of people domiciled in Colombia and subject to its jurisdiction remains to be seen.

References

Egan, Erin. 2019. "Data Portability and Privacy." Facebook. https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf

Newman-Pont, Vivian, and María Paula Ángel Arango. 2019 *Accountability of Google and Other Businesses in Colombia: Data Protection in the Digital Age.* Bogotá, Colombia: Dejusticia. https://www.dejusticia.org/publication/rendicion-de-cuentas-de-google-y-otros-negocios-en-colombia-la-proteccion-de-datos-digitales-en-la-era-digital/

ACCOUNTABILITY OF CDDBMs IN MEXICO

Milan Trnka Osorio

In this document, we review the privacy policies of four companies with data-driven business models (CDDBM) operating in Mexico, following the standards set in the report *Accountability of Google and Other Businesses in Colombia: Data Protection in the Digital Age* (Newman and Ángel 2019).

1. Selection of CDDBMs

From the "large Internet companies" category, which groups the five companies commonly referred to with the acronym GAFAM (Google, Amazon, Facebook, Apple, and Microsoft), we chose Amazon due to its presence in the Mexican market. The arrival of Amazon's services to Mexico was announced in July 2015 through its website (www.amazon.com.mx). It is considered the most ambitious launch of the company in 20 years (CNN Español 2015). Amazon's largest distribution centre for Latin America is located in Mexico (Milenio 2019).

As an intermediate company, we selected Snap Inc. and its product Snapchat. This platform offers social media services growing in popularity in Mexico, as shown by the ranking of the applications information and market company App Annie as per the top downloaded applications from Mexico's App Store and Google Play.[167]

In the start-up category, that is, companies defined for their early age, scalability, and exponential growth, we chose the company Payclip S. de R. L. de C. V. and its product Clip, which provides the user with the tools to make payments with their credit or debit cards from their mobile phone or tablet. At the time, the launch of this application was a

167. See https://www.appannie.com/en

significant breakthrough. It is considered one of the most successful start-ups in the country because of its practicality, ease of use, and because it sparked investors' interest, which led to a massive influx of capital from Silicon Valley to Mexico (Küfner 2018).

Finally, as an established company, we looked for the biggest company in the telecommunications sector. In the case of Mexico, this company is Radio Móvil Dipsa S.A. de C.V., the owner of the leading mobile carrier of the country and its product, Telcel.

Just like in the Report, there will be four analysis categories for each CDDBM to determine how they operate: 1) data sources, 2) processing, 3) purpose of data processing, and 4) relationship with GAFAM. Then, we will study how appropriate the Mexican legal regime is and evaluate the authority responsible for data protection.

2. Characterization of the CDDBMs' Operations

Based on a review of the privacy policies offered by the four companies included in the sample, below we analyze their operations based on the following four analysis categories: 1) data sources, 2) processing, 3) purpose of data processing, and 4) relationship with GAFAM. Annex 1 contains the systematization of this analysis.

2.1. Data Source

Both Amazon and Snapchat divide their data sources into three categories: 1) data provided by the user/customer, 2) information generated automatically as a result of the provision of the service, and collected through web tracking and crowdsourcing techniques, and 3) information collected from third parties. However, while Snapchat includes different sections related to its privacy policy, it is more understandable and more comfortable to read (Our Privacy Principles; Your Privacy, Explained; Privacy by Product; How We Use Your Information; and a Transparency Report. Furthermore, it provides a link to contact the area in charge of privacy and a dedicated cookies policy). For its part, Amazon only presents an example per type of information it collects from each source. Specifically, the five paragraphs explaining the information it collects use the phrase "for example" or similar five times (a clear breach of guideline 22 for privacy notices).[168]

168. Guideline 22: "The privacy notice shall specify the personal data that the controller will process to achieve the purposes for which data is obtained,

Payclip refers to the categories of information it collects rather than to the source of information. Therefore, it mentions that it collects, "including, without limitation," identification, computer, geolocation, and contact data (including, employment, commercial, financial, and patrimonial data), and third-party data. Payclip does not provide an exhaustive list of the data it collects, but instead presents an illustrative list of the different categories of information to which the data collected belong. The company is breaching the guideline by not being exhaustive and specific regarding the information obtained and, instead, being misleading and ambiguous by using phrases such as "including, without limitation," and using generic categories to refer to the data collected in the provision of the service. Again, this is a breach of Guideline 22 for the privacy notices mentioned above. Even though the privacy policy indicates that it does not collect sensitive data, this cannot be verified if it does not specify the data it collects.

Furthermore, due to the nature of the service, to provide users with tools to make payments with their credit and debit cards from their mobile phone or tablet, the Clip customer will manage the data of the third parties to which it provides the service or transfers the good they may charge through the application. According to the above, by accepting the privacy notice, Clip agrees to have its Privacy Notice establishing that its users authorize the transfer of their personal and sensitive data in its favour to process the data and fulfill the services between Clip and its customer. The client agrees to hold Clip harmless in case of a breach.

In turn, Radiomóvil Dipsa makes a distinction between personal data resulting from the service (which include identification and authentication, contact, patrimonial and/or financial, fiscal, demographic, device location, network and traffic data, and data on the user's preferences) and sensitive personal data, which, according to the privacy policy, are

---

both personally or directly collected from the subject, as those obtained indirectly through publicly accessible sources or transferred under the terms of article 15 of the Law. The controller shall comply with this content by identifying the personal data processed or its categories. The list of personal data, or its categories, shall not include inaccurate, ambiguous, or misleading phrases such as 'among other personal data' or 'for example.'" United Mexican States, Lineamientos del Aviso de Privacidad [Privacy Notice Guidelines], Secretariat of the Interior, January 17, 2013. México D.F.: Diario Oficial de la Federación. http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

"biometric data related to the fingerprints for identification purposes and confirm your identity to provide Services and the future transactions you make with Telcel."[169] Similarly, regarding the collection of data through indirect sources, whether through communications with affiliated companies or third parties with whom Telcel has commercial agreements or publicly accessible sources (including social media sites). Finally, it refers to third-party data it may collect and obtain from the user because, in some cases, a collateral is required to access a good or service.

2.2. Processing

As with the CDDBMs analyzed in the Report, the processing of personal data by the CDDBMs analyzed here also tend toward uniformity, focusing on two activities: collection and analysis. Regarding the data collection, four companies use similar tools:

- Cookies (proprietary and third party): these are small bits of information stored in the device to help websites and mobile applications remember specific things about the users when they revisit the site.
- Snap Inc.: to protect user data, acquire knowledge of the most popular features of the application and/or count visitors to a page, and offer more personalized services. They divide the cookies used into four categories: 1) necessary (to identify and prevent security risks); 2) preferences (to remember the settings and preferences, and improve the user's experience); 3) performance (information about the use of the site to monitor and improve its performance); and 4) marketing (deliver advertisement, ads, and specialized and relevant advertisement to the users according to their profile and interests).
- Amazon: allow users to access personalized service features and advertisements.
- Payclip: monitor the behaviour as an Internet user to offer a better service and user experience, and offer new products and services based on their preferences.
- Telcel: does not specify how it uses the information collected through these means.

169. Telcel, "Aviso de publicidad," 2019. Retrieved October 8, 2019, from https://www.telcel.com/aviso-de-privacidad

- Web beacons/Pixel tags: technology used in websites or in the body of emails to monitor certain activities.
- Web storage: local storage technology that allows the website to store data on a device's browser.
- URL: personalized web links that enable companies to understand the origin of their websites' traffic.
- Unique identifiers of applications and devices: chain of characters that may be used to identify a device, application, or browser exclusively.
- Sensors: internal mechanism of a device that enables it to measure and detect actions or external stimuli and act accordingly (accelerometer, gyroscope, barometer, magnetometer, proximity sensor, light sensor, thermometer, heart rate sensor, pedometer, fingerprint reader, etc.).

Regarding cookies as a means to collect information, it is noteworthy that Snapchat has its own Cookie Policy (effective from January 15, 2019). It offers the users of this platform with more information, specifically on technologies like cookies, web storage, and device identifiers. Similarly, it classifies cookies according to their use: 1) Necessary, 2) Preferences, 3) Performance, 4) Marketing, and provides the user with a small guide on disabling them in both the browser and the mobile device.

The analysis of the data collected is divided into two aspects. First, it seeks to personalize the service and segment users in groups with similar interests and connections (these may range from the contacts in the contact list, the places visited, the advertisements seen, or the products clicked); in other words, a descriptive analysis. Second, they make a prescriptive analysis to improve the user's experience to know the most popular features of the product or service. None of the four privacy policies specifies the technologies or methods used to perform this analysis.

For example, Telcel's privacy policy mentions that the purpose of the data collection includes:

> Processing with massive data analysis techniques to create profiles based on the combination of the information you provided, the information obtained from publicly accessible sources—including social media sites—and the information that might be inferred or obtained as a result of the application of various data analysis techniques.[170]

170. Telcel, "Aviso de publicidad," 2019.

Although the policy mentions an analysis technology, it does not describe it. On the other hand, Payclip's privacy policy specifies that one of the primary purposes is the "creation, integration, analysis, update and conservation of your file," again, without describing the technology used.

2.3. Purpose

The privacy policies of all the CDDBMs analyzed in this study mention similar purposes for the data collected. Generally speaking, these include confirming the user's identity, improving security, personalizing services and advertisements, creating profiles, and creating, updating, analyzing, and maintaining files, commercial prospecting analysis, and studies, sharing with third parties, etc.

In the case of Amazon, as mentioned above, this CDDBM does not provide an exhaustive list of the sources from which it collects its users' data, but only provides examples of the "type" of source from which it may collect information. Something similar happens in its purpose section. Again, this is a breach of the guidelines on privacy notices, which forbid generalities to describe the purposes of collecting and processing personal data.

Telcel is more precise. The company provides a particular list of the primary purposes for the data collected, mentioning the same general uses as in similar policies, which include verifying the identity, contacting the user, monitoring the customers' use of the products to improve and personalize them, complying with the obligation to cooperate with the security and justice entities (purpose specific to Telcel due to the nature of the service) and planning and performing dissociation procedures and create segregated audiences for third parties or commercial partners to offer their products or services. Regarding the secondary purposes of processing (which the user may request to opt out from), the policy mentions that they will use the data to inform the user of promotions, new products, or offers according to the profile and consumption habits created.

Payclip also divides the purposes of the data collected between primary and secondary. The primary purposes include those which are essential and necessary to provide the service, and the secondary purposes are those from which the user may opt out. Therefore, it refers to executing contracts to perfect the service provision, sending and receiving information from the "clip" readers, paying transactions, and issuing and sending documents confirming the transactions (invoices, receipts), as primary purposes.

Finally, in addition to its privacy policy, Snapchat has a special section explaining to the user how their information is used. The policy describes the development of the application as the principal and most important purpose. This means knowing the most used and accessible features for use as reference for future innovations. Likewise, it uses the information to personalize the service and the advertisements.

2.4. Relationship with GAFAM

None of the three companies studied here explicitly mentions any relationship with companies of the GAFAM group. However, some connections between them should be analyzed. First, both Clip and Telcel use "social media buttons," links embedded on websites to share information directly on social media sites. These buttons are part of the connection between two websites. The most common social media buttons are those linked to large companies, such as Facebook's "Like," Twitter's "Tweet," or Google+'s "+1."

Snapchat has its services linked to Google and Apple's maps and has the device's camera linked to Amazon. Its privacy policies are vague and unclear on this regard. As mentioned above, there is no reference nor direct mention to its relationship with the large companies; however, their connections are evident.

3. Evaluation of How Prepared the Personal Data Protection Legal Regime Is to Address the New Dynamics of the Digital Age

Considering how the companies studied here operate, now we will analyze the preparedness of the Mexican legal regime and the competent authorities to face the risks and hold these companies accountable regarding the processing of personal data in Mexico.

3.1. Scope of the Data Protection Regime

In Mexico, the right to the protection of personal data is a human right, enshrined in Article 15 of the Constitution of the United Mexican States (1917), which provides that:

> All people have the right to enjoy protection on their personal data and access, correct, and cancel such data. All people have the right to oppose the disclosure of his data, according to the law. The law shall establish exceptions to the criteria that rule the processing of data, due to national security reasons, law and or-

der, public security, public health, or protection of third party's rights.[171]

The Federal Law for the Protection of Data in Possession of Private Companies or Individuals[172] and the General Law for the Protection of Personal Data in Possession of Obliged Subjects were enacted as the laws to regulate this precept. Relevant to this analysis, below we will focus on the LFPDPPP.

The scope of application of the LFPDPPP includes all the natural persons or private legal persons engaged in personal data processing; this includes personal data controllers not physically located in Mexican territory.

Article 4 of the LFPDPPP regulations provides that the law is applicable even when the controller is not constituted in Mexican territory but is subject to the Mexican laws under an agreement or the terms of international law, and when the controller is not constituted in Mexican territory but uses means located there, except when said means are only used for traffic purposes and do not imply processing (Sections III and IV).

These provisions do not apply to: 1) credit information companies under the assumptions of the Law for the Regulation of Credit Information Companies and other applicable provisions; and 2) persons who collect and store personal data exclusively for personal use and without any disclosure or commercial use purpose (Article 2). In this regard, "processing" shall mean any "collection, use, disclosure or storage of personal data, by whatever means" (Article 3, sect. XVIII). Similarly, the "use" shall be interpreted as "any action to access, manage, exploit, transfer or distribute personal data" (Article 3, sect. XVIII).

According to Article 6, any processing of personal data shall be governed by the principles of legality, consent, information, quality, purpose, loyalty, proportionality, and responsibility (Article 6).

The law states, among other things, that personal data should not be obtained through misleading or fraudulent means and that there is a

---

171. United Mexican States, "Political Constitution of the United Mexican States," February 5, 1917. https://www.juridicas.unam.mx/legislacion/ordenamiento/constitucion-politica-de-los-estados-unidos-mexicanos

172. LFPDPPP, "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" [Federal Law for the Protection of Data in Possession of Private Companies or Individuals]. México D.F.: Diario Oficial de la Federación, July 5, 2010.

presumption of a reasonable expectation of privacy, that is, the trust that the personal data that any person provides to another will be processed per what the parties have agreed to in the terms established (Article 7).

Similarly, the law provides that, in the case of sensitive personal data, the controller shall obtain the subject's express and written consent to the processing, either through a handwritten or electronic signature, or any other authentication mechanisms established for such effects. No database containing sensitive personal data may be created without justifying its creation for legitimate and specific purposes and following the specific activities or aims pursued by the regulated person (Article 7).

According to the above, although it could be argued that the Mexican personal data protection regime is one of the most robust ones in comparison to other regimes in the region, the fact is that, given the increasingly changing and imminent technological advances, the existing scope of protection in this area is insufficient to deal with the potential risks or vulnerabilities arising from them.

Therefore, using the European General Data Protection Regulation (GDPR)[173] and the California Consumer Privacy Act[174] (CCPA) as an example given their scope of protection and how they provide for issues specific to the digital environment, below we address those aspects not yet provided for by Mexican legislation and whose implementation merits consideration.

3.1.1. What Is Not, but Must Be, Regulated

The definition of "personal data" in Article 3, section V of the LFPDPPP is quite similar to that of the Regulation and the CCPA. The law defines it as "any information relating to an identified or identifiable natural person."

---

173. 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

174. California Consumer Privacy Act (CCPA), 2018. Retrieved October 23, 2019, from https://oag.ca.gov/privacy/CCPA. Assembly Bill No. 375, Chapter 55, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy, approved by Governor on June 28, 2018.

3.1.2. Inferred Sensitive Data

The LFPDPPP recognizes "sensitive personal data" as "personal data which affects the most private sphere of the subject, or whose improper use may lead to discrimination or serious risk for the subject." Particularly, data "may disclose specific aspects such as racial or ethnic origin, current or future health status, genetic information, religious, philosophical and moral beliefs, membership to a union, political opinions and sexual preference" (Article 3, section VI).

However, the LFPDPPP fails to offer sufficient clarity on whether the above definitions include data inferred from other data; particularly, the inference of sensitive categories by aggregating non-sensitive data. While the CCPA does not refer to inferred sensitive data, Section 1798.140(o) explicitly mentions inferences made from various categories of data.

3.1.3. IP Address

Contrary to the developments of European law (Newman and Ángel 2019) and the explicit mention in the CCPA, the LFPDPPP does not explicitly mention online identifiers—such as IP addresses. This causes legal uncertainty and inconsistency in the processing of these data by CDDBMs. This practice, which at first might seem harmless, is an invasion of the users' privacy as IP addresses allow knowing the location from which a device accesses the network accurately; therefore, the IP address could be considered as personal data if the provider holds all the data required to associate that IP address to a specific person, knowing where they have been and the sites they have visited.

3.1.4. Automated Processing and Profiling

Similarly, the LFPDPPP falls short and does not offer explicit protection regarding any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, specifically, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health status, personal preferences, interests, reliability, behaviour, location, or movements. Moreover, unlike the Regulation, the LFPDPPP does not provide protection for data encryption (covered in Article 83 of the Regulation) nor for personal data systematic or large-scale processing (covered in Article 91 of the Regulation).

Furthermore, the Mexican State is even in breach of its obligation of issuing relevant regulatory legislation. Regarding commercial databases,

Article 42 of the LFPDPPP provides that the Secretariat of Economy shall issue regulations applicable to automated databases or databases that are part of an automation process. However, said regulations are yet to be issued as of the date of this report.

Further regulation to the rights of subjects regarding the automated processing of their personal data is particularly relevant for Mexico considering that the country was involved in the Cambridge Analytica scandal. This scandal involved a London-based defunct private company that "uses data analysis to develop campaigns for brands and politicians looking to change the behaviour of the audience" (BBC World, 2018). From March 19, 2019, several news reports revealed that the company acquired, presumably in an illegal manner, the personal data of around 50 million users through a Facebook application called "thisisyourdigitallife" (Cabrera 2017; Murata, San Martín, and Linares 2018).

The collection of such data is presumed to be illegal because, contrary to what Facebook stated, most users affected did not give their informed consent for their data to be exploited in this way, let alone for these purposes. Users ignored that by installing the application, they facilitated access to traits of their personality, mental health, sexual orientation, political views, substance abuse history, and other information that the pages they "liked" on the social media site could reveal (Tufekci 2017).

These data are sensitive personal data under Article 3 of the LFPDPPP; however, their automated processing and/or the profiling of their subjects are matters not yet explicitly covered by the law.

However, to date, no public evidence or information shows that the competent authority on the matter—the National Institute for Transparency, Access to Information and Personal Data Protection (INAI)—has sanctioned this practice in the country or even effectively implemented the corresponding verification process to investigate this case appropriately. Furthermore, there is no public evidence or information showing the efforts to extend the scope of protection of the LFPDPPP to the automated processing of personal data and/or unconsented, or even worse, inadvertent profiling of users, a situation that clearly violates the right to personal data protection.

3.1.5. Biometric Data

In addition to the above, unlike the Regulation and the CCPA, the LFPDPPP does not expressly include biometric data in its definition of sensitive personal data. Full and detailed regulation of data processing is crucial,

considering the degree of sensitivity, how unique it is to an individual, and the level of information that can be derived from such a category of data, since it includes, for example, data obtained from specific technical processing, relating to the physical, physiological, or behavioural characteristics of a natural person that lead to or confirm the unique identification of that person, such as facial images or dactyloscopy data.

To demonstrate the importance of regulating the processing of this type of data, the CCPA even develops this concept by including "physiological, biological or behavioural characteristics, including an individual's deoxyribonucleic acid (DNA), which can be used, singly or in combination with each other or with other identifying data, to establish individual identity."[175]

Biometric information includes, without limitation, images of the iris, retina, fingerprints, face, hand, hand palm, vein patterns, and voice recordings from which an identification template may be extracted, including a "faceprint," "*minutae template*," and typing patterns or rhythms, gait, sleep patterns, health status, or exercise information containing identification data.

In this context, it is crucial to mention that the potential use of biometrics in line with mass surveillance systems that can feasibly identify the data collected by the sensors around us is of particular concern. From such systems, it is possible to derive biometric patterns that, combined with the personal data collected from us daily, can give rise to databases that severely compromise anonymity (Chayka 2014) and the exercise of other rights.

In this regard, the United Nations Human Rights Council mentioned that the data collected for specific purposes are generally used for mass surveillance and, without sufficient legal and procedural safeguards, undermine human rights (UNHR 2014). Therefore, the LFPDPPP or its interpretation by the personal data protection authority must lead to clear and specific rules for processing this type of data.

175. State of California 2018, Assembly Bill No. 375, section 1798.140, para (b).

3.1.6. Other Relevant Personal Data of the Digital Environment

Furthermore, if we consider the CCPA, the LFPDPPP lacks a regulation that considers various categories of relevant data in the digital environment as personal data processing.

3.1.7. Commercial Information

This includes records of goods, products, or services acquired, obtained, or considered, or any other information on the purchase or consumption history or trends. This information is particularly relevant for CDDBMs offering goods and services. It allows for conducting more profound analysis based on its users' habits and explicitly allows creating profiles and segregating users according to their common interests. Based on this information, the company may direct specific advertisements to the users according to their online behaviour and determine their future behaviour.

3.1.8. Information of Activity on the Internet or Any Other Electronic Network

This category of information is usually considered to include, but not limited to, the browsing history, the search history, and information relative to the interaction of a consumer with a website, application, or online advertisement. The need for the LFPDPPP to expressly recognize and regulate the processing of this type of information as personal data is based on the fact that a compilation or analysis of this data may lead to infer traits of the subject's personality, mood, health status, sexual orientation, ideological, political and religious views, and other highly sensitive information that allows profiling and is usually sold or transferred to third parties, most of the time without the users' knowledge or consent, in a clear violation of the right to informational self-determination, among others.

3.1.9. Geographical Location

The recognition of a person's location data as personal data is particularly important, especially considering that under the Federal Telecommunications and Broadcasting Law—Articles 189 and 190, specifically—telecommunications companies are obliged to collect, store, and provide this information, even in real time, as required by the competent authorities. However, the legal protection of this information has been deficient, as shown by evidence based on public information. The access to this type of data by authorities not competent to make these requirements has been widespread (R3D 2018).

Even one of the companies with the largest share of telecommunications users in the country, Telcel, was found to be providing such information 100% of the time it was requested, without previously analyzing the origin or legality of the particular requirement (R3D 2018). This is of crucial importance considering that, as mentioned above, data revealing geographic location constitute highly sensitive data of a person. In this line, in Opinion 13/2011, the Data Protection Working Party created by Article 29 of Directive 95/46/CE of the European Parliament, clearly recognizes that location data disclose a large amount of sensitive information:

> A smart mobile device is very intimately linked to a specific individual. Most people tend to keep their mobile devices very close to themselves, from their pocket or bag to the night table next to their bed […]
>
> This allows the providers of geolocation-based services to gain an intimate overview of the habits and patterns of the owner of such a device and build extensive profiles. From a pattern of inactivity at night, the sleeping place can be deduced, and from a regular travel pattern in the morning, the location of an employer may be deduced. […] A behavioural pattern may also include special categories of data if it, for example, reveal visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations revealing data about, for example, sex life. These profiles can be used to make decisions that significantly affect the owner.

However, the LFPDPPP or any other current law of the country—and their interpretation by the competent bodies—do not define issues such as the procedure to obtain this type of personal data and do not recognize it as such nor regulate the processing of location data obtained or the safeguards required to detect and prevent the abuse of surveillance measures.

This contravenes the statement of the Supreme Court of Justice of the Nation (SCJN) in its resolution of Unconstitutionality Action 32/2012, by which it decided that the real-time geographic location of mobile communication equipment could only be considered constitutional if, among other things, it limited its use to exceptional situations for the investigation of particularly serious crimes defined in the law.

3.2. What Is Inadequately Regulated

Similar to the European Regulation, the LFPDPPP gives holders the power to exercise the following rights:

Article 23—Data subjects shall have the right to access their personal data held by the data controller and be informed of the Privacy Notice governing the processing is subject.

Article 24—The data subject shall have the right to rectify data if it is inaccurate or incomplete.

Article 25—At all times, the data subject shall have the right to cancel his or her personal data (Article 26: exceptions).

Article 27—At all times, and for any legitimate reason, the data subject shall have the right to object to the processing of his or her data. If applicable, the controller shall not process the data related to such a subject.

As mentioned above, although it could be argued that the Mexican legislation on the protection of personal data is one of the most robust in the region, the truth is that its scope of protection and the rights it confers on the personal data subjects continue to be quite limited to mitigate, react to, or compensate for possible damages or vulnerabilities inherent to the digital environment and the technological advances in this sense. If we take the European Regulation and the CCPA as a reference framework, it is possible to identify certain normative deficiencies concerning the LFPDPPP's intention to provide adequate protection. These include:

The right to data portability, that is, the right to receive the personal data concerning the data subject, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

Right to object the processing of personal data for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing.

The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The right to compensation for damages, whether of an economic nature or any other deemed relevant. The LFPDPPP still does not recognize the data subjects' right to receive compensation for material or non-material damages caused by the controller in violation of its obligations on the

matter. In this regard, based on the CCPA, the LFPDPPP should establish that any consumer will have access, at a minimum, to compensation for damages caused to him or her when his or her unencrypted or unreserved information is subject to unauthorized access, leakage, theft, or disclosure because the company fails to implement and maintain security measures and practices necessary to protect the information per its nature. To determine the appropriate amount of the compensation, the LFPDPPP should also provide that the competent court considers, for example, the nature and extent of the conduct incurred, the number of breaches, the persistence of the conduct, its duration, the intention to stop these actions, and the number of goods, degree of responsibility, and net value.

The right to be represented by a non-profit entity, organization, or association. The LFPDPPP also does not explicitly mention that a duly constituted non-profit entity, organization, or association may present the corresponding claim or exercise the rights vested by the law on behalf of the data subjects in the public interest and to protect rights and freedoms. Similarly, there are multiple obstacles to use the figure of "class actions" outlined in the Federal Code of Civil Proceedings in the case of violations to the right to data protection.

The right to opt out. Mexico has not given consumers the right to opt out from having their personal data sold to third parties by the companies who base their business on these actions.

The right to opt-in (applicable to minors). There has been no regulation to the processing a business or company must perform on the data of a consumer who is a minor when the processing consists of the commercial exploitation of data. It is understood that, under international standards on the subject, such a matter should be prohibited unless the consumer has the explicit consent of his or her parents or legal guardians and is over 13 years of age.

Notice of violation. It is essential for the LFPDPPP to recognize the subjects' rights to be notified of a violation when their personal data has been breached or compromised. Both the Regulation and the CCPA recognize this obligation by the data controller.

Transborder transfer of personal data. Unlike the Regulation, the LFPDPPP, lacks a provision stating that transborder transfers of personal data of subjects domiciled in the country may be performed only if the receiving third country or organization comply with the conditions established

by the law, thus ensuring an adequate level of protection and/or providing relevant safeguards for this purpose.

This issue is also particularly relevant considering the growing trend and/or international pressure for States to adopt international mutual assistance bilateral or multilateral treaties to provide the personal information of its citizens or inhabitants. If Mexico wants to be known as a country with an appropriate level of protection to receive this information, it will demand the same level of protection.

Robust legislation that considers the aspects mentioned above would help to address the problems derived from the harmful practices of the CDDBMs studied here. Thus, including new categories for the data collected, and considering them as personal data within a broad definition in the legislation would force the companies to be more specific when mentioning the data collected, as they could include them within the legal definitions provided by the law. Some issues can also be clarified, such as inferred sensitive data and automated processing and profiling.

3.3. Additional Considerations That Must Be Regulated

3.3.1. Best Practices Schemes

The LFPDPPP should promote the creation of certification mechanisms on data protection and data protection seals and marks to show that the controller has implemented adequate safeguards for the protection and transfer of personal data.

3.3.2. Registry of Processing Practices

Every controller should have records of its processing activities. The Regulation lists the information to be contained in the registry, including data transfers made to another country or international organization (Article 30).

3.3.3. Updating the Personal Data Category

Using the CCPA as an example, the regulations to update personal data protection to the additional data categories leading to changes in the technology and the collection practices or on obstacles for their implementation.

3.3.4. Regulation of the Right to Opt out from the Sale of Personal Data

The LFPDPPP should also establish rules and procedures to facilitate a consumer's request to exercise the right to opt out from the sale of their personal data. Similarly, to regulate that companies adequately safeguard the consumers' right to opt out from the sale of their personal data.

3.3.5. Balancing the Right to the Protection of Personal Data with the Right to Freedom of Speech and Information

Both the Regulations and the CCPA expressly mention that the right to the protection of personal data should be weighed against the right to freedom of speech and information. Given the level of interdependence of both rights, as well as the importance of harmonization between them, since by their very nature it is common for them to conflict without sufficient knowledge on the part of the legislators and the bodies of justice to make them coexist in the least harmful way possible, the LFPDPPP should incorporate this principle.

3.4. Scope of Territorial Application of the Personal Data Protection Law

The LFPDPPP does not mention its scope of territorial application; however, Article 4 provides said territorial scope, albeit very briefly, providing that the obligation to comply with the Mexican regulations on the matter will depend on the following assumptions:

- The processing is performed by a controller located in the Mexican Territory.
- The processing is performed by a processor on behalf of a controller located in Mexican territory, regardless of its location.
- The controller is not constituted in Mexican territory, but the Mexican legislation applies to it under a contract or the terms of international law.
- The controller is not constituted in Mexican territory and uses means located therein, except when said means are used solely for traffic that does not imply processing.

These assumptions are not explicit on whether the Mexican personal data protection regulations apply to companies located abroad but offering their services in the digital environment. Derived from the above, in practice, the interpretation of the INAI[176] has excluded any consideration related to the processing of personal data carried out by Internet companies such as Google from its competence, alleging a lack of territorial competence (El Informador 2017).

176. INAI Resolution to file number PPD 0094/14 dated January 26, 2015.

4. Evaluation of the Capacities of the Data Protection Authorities to Hold the CDDBMs Accountable

Article 6, section A(VIII) of the Constitution of Mexico provides the existence of an autonomous, specialized, impartial, and collegiate agency.[177] It must have a legal personality, own assets, full technical, managerial, and decision power over its budget and internal organization. It shall be responsible for guaranteeing the fulfillment of the right of access to public information and the protection of personal data held by obliged subjects. This body is the National Institute for Transparency, Access to Information and Personal Data Protection (INAI), comprised of seven commissioners appointed by the Senate of the Republic.

Regarding the private sector, the Federal Law for the Protection of Data in Possession of Private Companies or Individuals (LFPDPPP) establishes the powers of the INAI in its relationship with the processing activities performed by CDDBMs.

The LFPDPPP provides various mechanisms to safeguard the right to the protection of personal data. First, the law recognizes the rights to request a company to access, rectification, cancellation, or opposition (ARCO rights) regarding the relevant personal data. In the event of a disagreement with the answer given by the individual, the law provides for the Procedure for the Protection of Rights (PPD), which must be filed with the INAI and has the power to confirm, modify, or revoke the answer the company gave to the petitioner.

The INAI resolutions regarding the PPDs are appealable through a nullity trial before the Federal Court of Administrative Justice, whose resolutions are contestable through an *amparo* trial before the Judiciary of Mexico. In practice, this process may take years, undermining the effectiveness of this mechanism.

PPDs have been ineffective in remediating and dissuading practices that violate the right to personal data protection. For example, according to data obtained from the National Transparency Platform (INAI 2019), the INAI only received 251 PPD requests in 2018, of which only six resolved to revoke the answer of the company, and only 16 to amend it. In

177. United Mexican States, "Political Constitution of the United Mexican States," February 5, 1917. https://www.juridicas.unam.mx/legislacion/ordenamiento/constitucion-politica-de-los-estados-unidos-mexicanos

other words, in addition to the fact that the volume of requests is meager, only 8.7% of the PPDs were concluded and remedied a breach of the right to personal data protection. This is without considering the lengthy litigation before the Federal Court of Administrative Justice and the Judiciary of Mexico, which could imply an even lower number of definitive resolutions. These numbers contrast with the activity of other data protection authorities around the world. For example, the Spanish Data Protection Authority (AEPD 2019), operating in a country with about a third of Mexico's population, received 13,005 complaints (over 50 times the amount received by the INAI) and issued 11,830 resolutions, declaring a breach in 604 (27 times more than the INAI).

On the other hand, the INAI also has two other mechanisms to monitor and safeguard the right to personal data protection: the verification procedure and the sanctioning procedure. The verification procedure allows the INAI to open an investigation—ex officio or through a complaint—to determine whether a company complies with the LFPDPPP. For its part, the sanctioning procedure allows the INAI to sanction companies found in violation of the LFPDPPP, whether as a result of a PPD or a verification procedure.

Again, these procedures have not led to significant sanctions that allow considering a relevant dissuading effect. In 2018, the INAI solely imposed sanctions for little over 98 million Mexican pesos (approximately USD $5 million).

Therefore, although Mexico has a robust institutional design, with data protection legislation and authorities, in practice, there are severe obstacles for the effective enforcement of the right to the protection of personal data. Mainly, regarding the CDDBMs, there are interpretative limitations to apply the personal data protection mechanisms. In any case, there are significant obstacles for the eventual decisions of the data protection authority to become enforceable and be implemented quickly.

To provide an example and illustrate the reader on the preceding paragraphs, it is convenient to refer to the Ranking Digital Rights (2019) Corporate Accountability Index, a standard-setting tool aimed at encouraging online services companies, such as telecommunications companies, to comply with universal human rights standards that guarantee freedom of speech, privacy, and the use of personal data.

The report, published in May 2019, evaluated the company América Móvil—of which Telcel is part—as it is one of the largest

telecommunications companies in the world and the largest in the region. According to the evaluation, despite progress in its behaviour regarding its users' freedom of speech and right to privacy, in addition to publicizing new training for workers and programs on alerts and human rights, it still falls short of the primary benchmarks on transparency.

For example, the company does not publish information on how it manages government and private requests to block content or give information about its users. Likewise, it failed to provide sufficient information about its policies that affect privacy and security. Furthermore, it does not clarify whether it notifies its users when the authorities request personal information (despite having the legal obligation to do so).

Finally, Telcel did not provide information related to eventual massive data leaks. Although the companies in Mexico have the obligation of notifying its users when it "significantly affects" their rights, Telcel does not disclose this information to its users. América Móvil had a rating of 25 out of 100, far from being the best company in the sector, Telefónica (Spain), with 57.

Recommendations

The Mexican personal data protection regime is insufficient to ensure the accountability of CDDBMs. Therefore, the regulatory and institutional framework must be adapted to ensure that these companies' growing sophistication of personal data exploitation practises does not leave individuals and society in general defenceless against their multiple impacts.

We suggest the following to fix the shortcomings of the Mexican personal data protection regime:

1. Extend the regulatory and/or interpretative scope of the right of access so that data subjects, academia, enforcement bodies, and society in general can know, identify, study, and discuss the impacts of the exploitation of personal data by the CDDBMs on human rights. Particularly:
    a. The right of access, established in the LFPDPPP, should be amended or reinterpreted so that the right to know the "generalities of the processing" does not prevent the relevant actors from knowing the sources, purposes, processing, and transfers made from the exploitation of personal data with further detail.
    b. The body in charge of safeguarding personal data protection must adopt a broader interpretation of the concept and use its

verification powers more efficiently to create more knowledge on how the CDDBMs operate.

c. More academic research on the scope and repercussions of the CDDBMs on human rights in Mexico should be promoted.

2. A more significant regulatory and interpretative development of crucial concepts to ensure the protection of personal data and respect for other human rights should be promoted based on the practices of the CDDBMs. Particularly:
   a. The concepts of "personal data" and "sensitive personal data" should be clarified to include, at least in some circumstances, biometric data, online identifiers, or other unique device identifiers.
   b. There must be protection regarding the inference of sensitive categories from the aggregation of non-sensitive data.
   c. Develop specific limitations and protections regarding the use of online monitoring techniques, such as cookies and pixel tags, among others.
   d. Develop specific limitations and protections regarding practices such as profiling, to ensure transparency, informational self-determination, and prevent discrimination.
   e. Develop specific limitations and protections regarding automated decision-making and its consequences. At least ensure that the individual has the right to know when an automated decision affects him or her, or to know specificities regarding the process and the result of the decision.
   f. The ambiguities regarding the notification obligations in case of security breaches should be notified. Specifically, the law should provide the obligation of notifying the INAI of any breach and not limit the notification obligation to the data subject only regarding the breaches which "significantly affect the moral or patrimonial rights," as currently provided in Article 20 of the LFPDPPP.
3. Considering the power asymmetry and the intrinsic powers to people's capacity to give informed and free consent, there should be limits to the consent to the processing of personal data representing an affectation to the public interest.
4. Amend the regulatory norms of the LFPDPPP and the interpretation of the INAI regarding the territorial scope of the law, so that

CDDBMs who despite being domiciled outside the country offer services that affect the exercise of the right to data protection of users located in Mexico must comply with the provisions of the LFPDPPP.

5. Strengthen the institutional capacities to enforce the right to the protection of personal data. Some measures to be considered include:
   a. Strengthen the capacities of the INAI as personal data protection regulator, ensuring sufficient material and human resources to perform its duty.
   b. Eliminate the possibility of contesting the INAI's decisions before the Federal Court of Administrative Justice and only offer an *amparo* trial as a means for judicial control of the regulator's decisions.
   c. Remove obstacles to exercise the verification powers and increase the amount of the sanctions the INAI may impose, so the verification, protection, and sanctioning processes are truly dissuasive of conducts that violate the right to the protection of personal data.
   d. Enable the INAI to order effective compensation mechanisms for the subjects of the right to the protection of personal data affected by violations to the LFPDPPP.
   e. Encourage universities to develop capacities and promote specialized education on the protection of personal data in Mexico.
   f. Promote the cooperation between the data protection authorities and other national and international authorities.
6. The CDDBMs must implement adequate self-regulation measures to prevent, avoid, mitigate, or correct any impact on the right to the personal data protection, including the minimization of personal data processing and effective anonymization measures resilient to reidentification measures and effective transparency measures, among others.

References

AEPD. 2019. "Memoria 2018." Spanish Data Protection Agency. https://www.aepd.es/media/memorias/memoria-AEPD-2018.pdf

Article 29 Working Party. 2013. Opinion 03/2013 on purpose limitation. Adopted April 2, 2013, 00569/13/EN WP 203, 45. https://ec.europa.eu/

justice/article-29/documentation/opinion-ecommendation/files/2013/wp203_en.pdf

BBC World. 2018. "5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día." March 21, 2018. https://www.bbc.com/mundo/noticias-43472797

Cabrera, Rafael. 2017. "Esta empresa que ayudó a la campaña de Trump ahora busca personal para las elecciones en México." *BuzzFeed News,* October 31, 2017. https://www.buzzfeed.com/mx/rafaelcabrera/esta-empresa-que-ayudo-a-la-campana-de-trump-ahora-busca#.idgaM5x7X

Chayka, Kyle. 2014. "Face recognition software: Is this the end of anonymity for all of us?" *The Independent*, April 23, 2014. https://www.independent.co.uk/life-style/gadgets-and-tech/features/face-recognition-software-is-this-the-end-of-anonymity-for-all-of-us-9278697.html

CNN Español. 2015. "Amazon llega por primera vez a América Latina abriendo una tienda digital en México." https://cnnespanol.cnn.com/2015/07/01/amazon-llega-por-primera-vez-a-america-latina-abriendo-una-tienda-digital-en-mexico/

El Informador. 2017. "Vacío legal impide aplicar el derecho al olvido en México." *El Informador*, February 5, 2017. https://www.informador.mx/Tecnologia/Vacio-legal-impide-aplicar-el-derecho-al-olvido-en-Mexico-20170205-0093.html

Entrepreneur. 2019. "Estas son las 10 startups mexicanas más populares en LinkedIn." *Entrepreneur*, September 4, 2019. https://www.entrepreneur.com/article/339056

Küfner, Sabine. 2018. "Clip : La evolución de la Startup más exitosa de México." *Medium*, May 14, 2018. https://medium.com/newco-shift-mx/clip-la-evoluci%C3%B3n-de-la-startup-m%C3%A1s-exitosa-de-m%C3%A9xico-d520bdc6ef51

Milenio. 2019. "Amazon abre en México su centro de distribución más grande de Latinoamérica." *Milenio*, July 31, 2019. https://www.milenio.com/negocios/amazon-abre-mexico-centro-distribucion-grande

Murata, Gloria, Neldy San Martín, and José Raúl Linares. 2018. "Los 'gurús de datos de Trump' están en México y nadie sabe qué diablos hacen." *El Financiero*, January 23, 2018. https://www.elfinanciero.com.mx/nacional/los-gurus-de-datos-de-trump-estan-en-mexico-y-nadie-sabe-que-diablos-hacen

INAI. 2019. "Información estadística : Procedimiento de Protección de Derechos correspondiente al primer trimestre de 2018." National Transparency Platform. https://consultapublicamx.INAI.org.mx/vutweb/faces/view/consultaPublica.xhtml#obligaciones

Newman-Pont, Vivian, and María Paula Ángel Arango. 2019. *Accountability of Google and Other Businesses in Colombia: Data Protection in the Digital Age.* Bogotá, Colombia: Dejusticia. https://www.dejusticia.org/publication/rendicion-de-cuentas-de-google-y-otros-negocios-en-colombia-la-proteccion-de-datos-digitales-en-la-era-digital/

R3D. 2018. "Transparencia y Vigilancia en México, Lo que no sabemos sobre lo que el gobierno sabe de nosotros." México: Red en Defensa de los Derechos Digitales. https://r3d.mx/wp-content/uploads/r3d-transparenciayvigilancia.pdf

Ranking Digital Rights. 2019. "2019 RDR Corporate Accountability Index." https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019report.pdf

Tufekci, Zeynep. 2018. "Facebook's Surveillance Machine." *New York Times*, March 19, 2018. https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html?referer=https://t.co/wZEheBtu4U%3famp=1

UNHR. 2014. "The Right to Privacy in the Digital Age." A/HRC/27/37, June 30, 2014. Geneva, Switzerland: United Nations High Commissioner for Human Rights. https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

CDDBMs AND PERSONAL DATA PROTECTION IN BRAZIL, CHILE, COLOMBIA, AND MEXICO: THE COMMON EXPERIENCE

Daniel Ospina-Celis
Juan Carlos Upegui

In this chapter, we present an analytical and comparative overview of how some CDDBMs collect and process personal data in Brazil, Chile, Colombia, and Mexico. This exercise is possible thanks to the country reports included in this book. According to the methodology described in the introduction of each chapter, the reports were prepared based on an analysis of the privacy policies of the products offered by various companies and their relationship with the Internet giants (GAFAM). As a comparative exercise—and by highlighting the common findings—this chapter intends to account for the challenges that the advances of the digital era pose to the rights to the protection of private life and personal data in the region.

At the same time, this comparative report is a reflection on the current dynamics of the digital age and their impact on fundamental rights, a brief exercise in comparative law—in terms of local legislation on personal data protection—and a modest contribution to the literature on the relationship between business and human rights[178] in digital environments.

178. Developing this idea, the United Nations Human Rights Council adopted the Guiding Principles on Business and Human Rights: United Nations General Assembly, Resolution A/HRC/RES/17/4, "Human Rights and Transnational Corporations and Other Business Enterprises," July 6, 2011. https://undocs.org/en/A/HRC/RES/17/4. The Guiding Principles on Business and Human Rights are contained in United Nations, HR/PUB/11/04, 2011, "Implementing the United Nations 'Protect, Respect and Remedy' Framework." New York and Geneva: United Nations. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf

The right to the protection of personal data is a human right derived from the right to privacy. In the global context, the right to the protection of privacy was recognized under Article 12 of the Universal Declaration of Human Rights[179] and Article 17 of the International Covenant on Civil and Political Rights.[180] Interpreting these provisions, the Human Rights Committee mentioned that "every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes."[181] In 2016, the United Nations General Assembly adopted Resolution A/C.3/71/L.39 on the right to privacy in the digital age, which calls upon all States and business enterprises to meet their responsibility of respecting human rights, including the right to privacy in the digital age.[182]

In the European context, the right to the protection of personal data was the subject of the Council of Europe Convention 108 of 1981, the first international instrument whose purpose was to safeguard every individual's "right to privacy, with regard to automatic processing of personal data relating to him."[183] Similarly, it was recognized as an autonomous fundamental right under Article 8.1 of the European Union Charter of Fundamental Rights, adopted in 2000—and binding since 2009—as the right of every individual "to the protection of personal data concerning him or her."[184] In turn, in the context of the European community law, in 1995, it adopted Directive 95/46/CE of the European Parliament and of the Council, which extensively regulated the "protection of persons

---

179. United Nations General Assembly, "Universal Declaration of Human Rights," Paris, 1948. https://www.un.org/en/universal-declaration-human-rights/

180. United Nations General Assembly, "International Covenant on Civil and Political Rights," New York, 1966. https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

181. Human Rights Committee, General Comment No. 16 of 1988, General Comments Adopted by the Human Rights Committee, Article 17. 1988. https://undocs.org/en/HRI/GEN/1/Rev.7

182. United Nations General Assembly, Resolution A/C.3/71/L.39, "The Right to Privacy in the Digital Age." October 31, 2016. https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx

183. Council of Europe, Convention 108 of 1981, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. January 28, 1981. https://rm.coe.int/16806c1abd

184. European Union, "Charter of the Fundamental Rights of the European Union." Official Journal of the European Communities, C 364/1. December 18, 2000. https://www.europarl.europa.eu/charter/pdf/text_es.pdf

with regard to the processing of personal data."[185] Recently, this directive was revoked by the new General Data Protection Regulation, Regulation (EU) 2016/79, which updated the personal data protection regime to bring it in line with the new practices of the digital economy.[186]

In the Latin American sphere, there is still no binding international instrument that recognizes and regulates the right to personal data protection. However, it has been recognized in soft law instruments, such as the Declaration of Santa Cruz de la Sierra,[187] adopted in 2003 at the end of an Ibero-American summit of Heads of State which, in numeral 45, recognizes the protection of personal data as a "fundamental right of people." Furthermore, in 2017, the Ibero-American Data Protection Network passed the "Standards for Data Protection for the Ibero-American States," recognizing the protection of personal data as a fundamental human right (recital 1), especially relevant in the digital age.[188]

Parallel to the developments on the right to the protection of privacy at a global and regional level, the legal systems of the countries under analysis have constitutionally and legally recognized the right to data protection. In Brazil, the right to habeas data is recognized under number 71 of Article 5 of the 1988 Constitution.[189] Specifically, it safeguards a procedural mechanism to know the information regarding an individual contained in public databases and for data rectification. Law 13.709 of

---

185. European Parliament and Council, Directive 95/46, "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data." October 24, 1995. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

186. 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

187. Organization of American States, "Declaration of Santa Cruz de la Sierra," Andean Presidential Council, January 30, 2003. https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf

188. 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

189. Constitution of the Federative Republic of Brazil, October 5, 1988. https://www.acnur.org/fileadmin/Documentos/BDL/2001/0507.pdf

2018, which extensively regulates personal data protection, was enacted in Brazil almost 30 years after the enactment of the constitution.[190]

Just like Brazil, Article 15 of the Political Constitution of Colombia of 1991 recognizes every individual's right to know, update, and correct the personal information contained in public or private data banks.[191] In the development of this proposition, 20 years after the constitutional reform, the Colombian Congress passed Law 1581 of 2012, a general regulation on the right to personal data protection.[192]

In Chile, the right to personal data protection was included in 2018's constitutional reform, including it under number 4 of article 19. According to this article, all people have the right "to the protection of personal data." The processing and protection of these data will be carried out in the form and under the conditions determined by law. However, more than 20 years ago—in 1999—the Chilean Congress passed Law N° 19.628, one of the first laws to regulate personal data protection in the region. Given the antiquity of the Chilean regulation, the new constitutional reform, and the technological advances since 1999, the Chilean Congress is debating an update to its data protection regulations.

Since 2009, Article 16 of the United Mexican States' political Constitution expressly recognizes the right to personal data protection, access, correction or cancellation, and to express their opposition to the processing of personal information. Out of the four constitutional provisions mentioned, the latter is the most complete and comprehensive. From this constitutional reform, the Federal Law on the Protection of Personal Data in Possession of Private Parties or Individuals was enacted in 2010.

Considering that personal data protection is an internationally recognized human right and a fundamental constitutional right for the States analyzed in this study, this chapter intends to identify some characteristic or relevant elements of the data collection and processing practices by CDDBMs domiciled in Brazil, Chile, Colombia, and Mexico. Second, it

---

190. Government of Brazil, "Lei Geral de Proteção de Dados Pessoais" [LGPD; Personal Data Protection Law]. Law 13.709, August 14, 2018. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

191. Political Constitution of Colombia, July 7, 1991. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

192. Statutory Law 1581 of 2012, "Whereby general provisions for the protection of personal data are issued." October 18, 2012, D.O. 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

intends to identify how the local legislation of these countries regulate (or not) these practices, and whether the regulation is adequate and sufficient. Finally, we make some recommendations that can be used as an input for a future regional regulation that strengthens the protection of rights related to the processing of personal data and leads to accountability by the CDDBMs collecting and processing the personal data of citizens in the region.

For these purposes, we will first analyze the common aspects in the operations of the CDDBMs, which also implies identifying the risks the four countries face regarding the use and analysis of data in the digital age. We will then analyze the regulatory shortcomings of the relevant legislation regarding the processing of personal data in the digital age and its technological developments. Finally, we will analyze the figure of the data protection authority and its capacities to hold CDDBMs that violate the legislation accountable.

1. Standard Aspects and Risks of CDDBMs Operations

The country studies on the practices of the CDDBMs show some convergence in how these companies collect data and analyze the reasons and practices with which they process personal data in the context of the digital economy, even though each company processes the personal data of its users/customers based on its business strategy. Below we will present the familiar aspects to most of the CDDBMs analyzed—over 40 companies—operating in Brazil, Chile, Colombia, and Mexico, and their implications for the right to personal data protection of the digital services' users. For this, we will consider the categories defined in the research methodology: 1) data sources, 2) processing, and 3) purpose of processing.

1.1. Data Sources

Most of the CDDBMs analyzed recognize that they collect their users/customers' data from three sources: 1) data provided directly by the user/customer, 2) data collected through web tracking or monitoring, and 3) data provided by third parties or strategic partners. These three sources are typical of the digital economy. For example, in Mexico, Amazon and Snapchat openly recognize in their privacy policies that they use these three categories as data "sources."

1.1.1. Direct Collection from the Source: Data Subject Registry

The data provided by the user/customer is usually collected during registration in the platform and, therefore, is data on which the subject has higher possibilities of knowledge, control, and influence in its collection. The CDDBMs studied usually request the creation of an account or profile to use the product/service they offer. This is the case for iFood and Magazine Luiza in Brazil; AIRA, Facebook, and PedidosYa in Chile; Facebook, Instagram, Uber, and others in Colombia; and Amazon, Snapchat, and Payclip in Mexico. In all these cases, the applications or services cannot be used without creating a profile. The data usually collected this way are: name, email address, age, telephone number, postal address, and payment data—credit card number, franchise, etc.—in the case of the CDDBMs engaged in selling and delivering goods and services.

Little Clarity on the Type of Data Collected

A common circumstance of the privacy policies of the CDDBMs analyzed in the four countries is that few of them exhaustively mention the data they collect. In Mexico, Payclip's privacy policy mentions that it collects a list of data as an example but without limitations; in turn, Amazon's privacy policy uses vague and ambiguous terms and incurs in the practice—forbidden by the Mexican guidelines on privacy policies[193]—of using examples of the data collected without exhaustively mentioning the list of data collected. Above all, this practice shows a lack of transparency on all the personal data effectively collected and the impossibility of the data subject of, first, knowing which personal data will be processed and, second, exercising any control on subsequent processing.

Brazil has one of the most concerning cases in this aspect. Upon studying Amazon Prime Video's streaming service, sold through the subscription of a contract with Vivo, a telecommunications company and Telefónica affiliate, the study showed the concurrence of two privacy policies (Vivo's and Amazon Prime's) with the aggravating circumstance that,

---

193. The privacy notice guidelines are an administrative act issued by the Mexican data protection authority (INAI), which sets standards to establish the privacy policy by obliged subjects under the Law for the Protection of Personal Data Held by Private Parties. United Mexican States, Lineamientos del Aviso de Privacidad [Privacy Notice Guidelines], Secretariat of the Interior, January 17, 2013. México D.F.: Diario Oficial de la Federación. http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

in the case of the latter, the policies are only available in English. Both privacy policies apply to the user, but it is not very clear what happens in case of inconsistencies between them. In this case, the size of the pool of personal data collected is unclear, the average consumer has difficulties finding the applicable privacy policy, and only a qualified consumer—with sufficient time and knowledge of the English language—could have a more or less accurate idea of the type and extent of the data being collected.

Sensitive Data

Some CDDBMs request information which, according to the legislation of each country, are sensitive data.[194] In general, sensitive data have special protection, as they are considered a special category of personal data because they pertain to people's most intimate sphere and their improper processing could lead to discrimination. Usually, this is information related to the religious beliefs, political views, physical or moral characteristics, habits (in the Chilean case), biometric and health-related data, among others. The case of "habits" is noteworthy. User/customer profiling and loyalty are critical activities for CDDBMs. None of these essential digital economy assets may be obtained or traded without processing personal data on the consumption or behaviour "habits" of customers/users. The matter is so delicate that the elimination of "habits" as a sensitive data category has been proposed as part of the discussion of the new Chilean data protection regime. The experts consulted on the Chilean case consider this as an apparent regression from the existing legal regime. The matter is critical, as CDDBMs are clearly interested in this type of information not being considered sensitive. In Colombia, Tinder and Unilever expressly mention and require providing sensitive information during sign-up. On the other hand, EasyTaxi's privacy policy—also in Colombia—expressly mentions that "none of the data that will be processed is considered as sensitive." This could be considered good practice, as the company voluntarily refrains from collecting sensitive data, understanding that it is not required to provide the service.

---

194. In Chile, sensitive data are regulated under Law N° 19.628, article 2(g); in Colombia, they are regulated under Law 1581 of 2012, Article 5. Mexico regulates sensitive data through the Federal Law for the Protection of Data Held by Private Parties, Article 3(VI), and Article 9. Finally, in Brazil, the processing of sensitive personal data is regulated under Article 5(II) and Articles 11, 12, and 13 of Law 13.709 dated August 14, 2018.

"Necessary" Data

Data protection legislation in Brazil, Chile, Colombia, and Mexico do not directly or explicitly regulate the voluntary provision of personal data in the digital environment. These actions are regulated by the general regulations on consent to use and collect data and by the necessity & proportionality principle. CDDBMs must adequately inform the data they collect and ensure that the user provides it voluntarily, especially regarding sensitive personal data. The cases of Facebook and Falabella's policies of use in Chile become relevant because they force the user to provide information on sex/gender as a requirement to use the service. Is providing this data to Facebook or Fallabella *necessary* to use the social media site or the retailer's online service? Or is this a disproportionate requirement by the CDDBMs, which many users are willing to accept as long as they can use Facebook or Falabella's online services? Some sign-up processes do not make any distinction between the different types of personal data (sensitive/non-sensitive) or do not give the user freedom to opt out from providing sensitive data and the argument that justifies their collection is the "personalization of communications" (according to their policy, the messages are different for men and women) seems insufficient. This situation is an example of the unbalance between the company and the user, even in a scenario of ostensible free consent.

Payment-Related Data

Another type of data usually collected and provided directly by the user/customer is the information required to make payments and other transactions through the platform. CDDBMs collect data such as the bank name, account number, and/or user's credit card number, franchise, expiration date, etc., to facilitate entering into purchase agreements through their platforms. Similarly, they may collect information related to the products selected, purchase history, mailing or shipping address, and the amount of the transactions. It is very concerning that companies engaged in the sale or intermediation and which, due to the nature of the service provided, collect information on purchases and transactions, are not entirely transparent. Falabella and PedidosYa, two platforms that offer goods and services in Chile, do not express that they collect this information in their privacy policy. This is in contrast with iFood (Brazil)[195] or Facebook's

195. iFood, "Privacy Policy," 2018. https://www.iFood.com.br/privacidade

terms of service which state that these companies process "payment information, such as your credit or debit card number."[196]

1.1.2. Data Collection Through Web Tracking

Regarding the data collected through web tracking or monitoring, that is, information on the Internet systems and tools a user utilizes to browse or use a platform, the situation requires an especially technical assessment. This dimension of collection mainly includes information on the application's activity (called online data), which refers to data such as time of use of the application, purchase information, search history, mouse heatmap, and interactions in the platform. It also includes information on the devices or systems used by the user (log data), such as the application, the IP (Internet Protocol) address to establish the connection, the type of device, the network the user is connecting to, the browser's version, and language or time zone preferences.

The main characteristic of this data source is that the information is collected every time the user opens the application or visits the website; therefore, it may indicate user/client/customer patterns or habits of interest to the CDDBMs. Thanks to the data collected through web tracking, where in principle there seems to be no collection of personal data, companies can profile their users and offer personalized services. In the cases of Chile and Colombia, Facebook is the company that best describes its monitoring methods. It categorizes the data obtained according to the mechanisms used: 1) device attributes, 2) device operations, 3) identifiers, 4) device signals, 5) data from device settings, 6) network and connections, and 5) cookie data.[197]

Web Tracking and Cookies

Web tracking refers to collecting information (including personal data) created by browsing on the Internet. In principle and appearance, the information is not personal, but it is insofar as it can be linked to an identifiable person employing a user ID. The information collected is not necessarily produced during the interaction with the website, but may correspond to information specific to the device used to browse on the website. Note that the system needs to identify the device because it

196. In this regard, see the section "Information about transactions made on our Products" of Facebook's privacy policy at https://www.facebook.com/policy

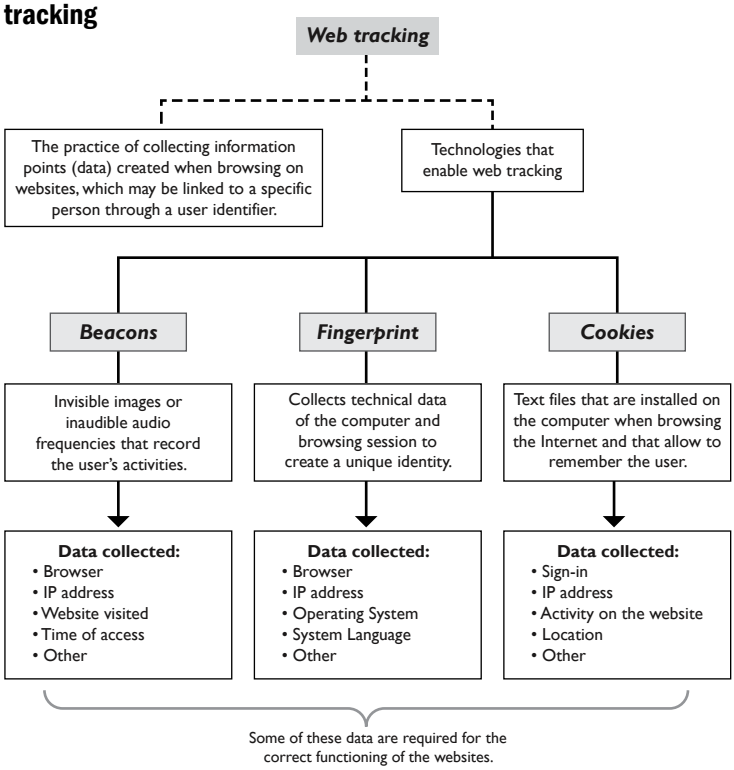
197. See https://www.facebook.com/about/privacy/update

allows for facilitating the browsing experience. For example, this allows a website to display the users' language, maintain the active session when browsing on a social media site, or save the products sent to the shopping cart when starting the online payment process.

Several tools may be used to perform web tracking. These tools will collect information depending on their characteristics. Generally speaking, there are two types of web-tracking technology: stateful web tracking and stateless web tracking. The first implies installing a file in our devices, whereas the second is based on the collection of information (usually the device's technical data), without installing any file whatsoever. Cookies are an example of stateful technology, while the fingerprint and beacon are stateless technology. Figure 1 explains web tracking and some of its enabling technologies.

We will now make a brief reference to cookies as specific tools for web tracking. Despite the relevance of other technologies used for web tracking, we will only discuss cookies because of their relevance to the privacy policies discussed in this book.

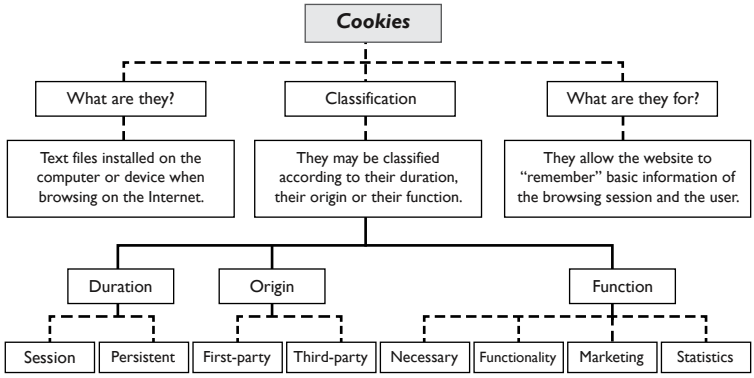
Figure 1
Web tracking



Cookies are small text files installed on the devices while browsing on the Internet. Their primary purpose (and their first use) was to facilitate a user's browsing as they "remember" specific information useful for websites. For example, they allow the site to recognize that the user logged in or selected a particular option/setting. Nowadays, cookies are used for much more than allowing adequate browsing through the websites. One of their most common uses is the collection of personal information for advertisement or marketing purposes.

Cookies can be classified using three criteria: 1) their duration, 2) their origin, and 3) their purpose. Regarding their duration—that is, how long they remain on a device—cookies may be session (deleted upon closing the browser or signing out) or persistent (remain after closing the browser until deleted or expired). If we consider their origin, cookies may be first-party or third-party cookies. Upon visiting a website, it installs first-party cookies, whereas a different actor installs third-party cookies to the website on which we are browsing. Finally, regarding their purpose, cookies may be necessary (browsing is impossible without them, e.g., online shopping), functional (they improve the browsing experience, e.g., recognize the language), statistical (add data on how the website is used), or marketing (seek to adapt the advertisement shown to the user). Figure 2 shows a visual representation of cookies and their classification.

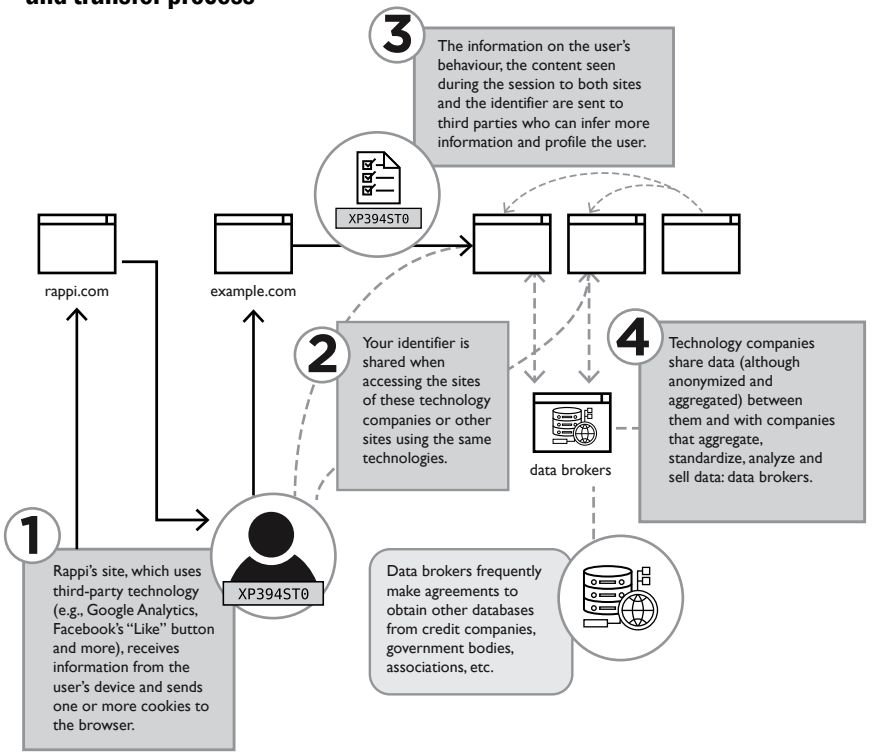
Figure 2
Representation of cookies functioning



This is framed within a context in which, as shown by the practices of the CDDBMs analyzed, companies share data between them and data

companies or data brokers. Figure 3 shows a graphical representation of the data collection process in websites and the transfer of data between companies.

Figure 3
Graphical representation of the data collection and transfer process



Status of the Data Obtained Through Web Tracking

Understanding the nature (personal or otherwise) of the data obtained through web tracking is critical in the context of data collection practices. For example, the Brazilian company iFood, a food delivery application, estimates that the information on their users' activity in the company's website or application is not personal, as it is aggregate and supposedly does not allow identifying every user. The policy also states that "the age, preferences, language, cep and the area code" of a user are "non-personal data."[198] A similar situation happens in the case of Social Miner, Brazil's digital marketing start-up. Its privacy policy denies the

198. iFood, "Privacy Policy," 2018

condition of personal information of the data collected through persistent and session cookies when they are used for general market studies. Social Miner states that "the data used for general behaviour studies is obtained by deleting the user's personal information." In this case, these data are no longer personal but a "set of anonymized data collected for study and research." The definition of the data collected through web tracking as non-personal information is not exclusive to the Brazilian companies. In Colombia, Duety and Apple claim that these data are not linked to the user/customer, but to an IP address.

Processing and Cookies

The privacy policies of the companies studied in Brazil, Chile, Colombia, and Mexico usually mention that they use cookies to collect users' information. Cookies are a discrete source to collect personal data. Their relevance is such that several CDDBMs have decided to refer to the purpose and type of information collected from cookies. They are so crucial for the companies analyzed—and for big data in general—that several of them have their own cookies policy, separate from their privacy policy. This is the case for Snapchat in Mexico, PedidosYa in Chile, and Social Miner in Brazil. Due to the prevalence of collecting data through cookies, these companies created a document exclusively aimed at explaining how their products' cookies work to their users. Similarly, Facebook's data policy has a section devoted to explaining cookies and other storage technologies in detail.

For example, in Mexico, Snapchat's privacy policy mentions that it uses cookies for various purposes (security, personalization, performance), and classifies them into four categories: 1) necessary (to identify and prevent security risks), 2) preferences (to remember the settings and preferences, and improve the user's experience), 3) performance (information about the use of the site to monitor and improve its performance), and 4) marketing (deliver advertisement, ads, and specialized and relevant advertisement to the users according to their profile and interests). In turn, in its cookies section, Chile's PedidosYa explains in detail that it uses three types of cookies: analytical, session, and persistent, and mentions that these collect "information about your computer and your visits and use of this website, including your IP address, geographical location, browser type, source of the traffic to the type, duration of the visits and number of visits per site."

1.1.3. Data Provided by Third Parties

The data provided by strategic partners or third parties are the third source of data the CDDBMs analyzed use. Considering how the personal data market works and its relevance for the digital economy, it could be assumed that companies openly acknowledge that they obtain data from third parties and that they inform the user/customer of this situation. However, this is not the case in reality. Out of the four CDDBMs analyzed in Chile, only Facebook recognizes in its privacy policy that it collects data through strategic partners, which are thousands around the world due to its nature as a large Internet company and the possibility of linking virtually any page or platform with social media buttons. This implies that the other companies studied in Chile either do not use data provided by third parties or at least are not transparent about it. On the other hand, there are good examples of transparency in this point, such as the application 8fit Workouts and Meal Planner in Colombia, which include the names of all third-party applications that connect to the app and the partners with whom it shares information.

Data Collection Outsourcing: A Transparency Issue

Although collecting data through partners or third parties does not necessarily imply a legality issue in the strict sense (although it might be), it does suggest a generalized lack of transparency by the CDDBMs studied. For example, in Colombia, Spotify's terms of service provide that the company will use personal data when a third party has been authorized or whenever the company has a legitimate interest in using it. Who are the strategic partners on which CDDBMs rely to collect data? This type of information is not usually available in privacy policies. Another example of this is Mexico's Telcel. In its privacy policies, the company recognizes that it may collect data from indirect sources, such as communications with others or third parties with whom Telcel has commercial agreements; the company may even collect personal data from publicly accessible sources (such as social media sites). However, the privacy policy does not mention the commercial partners from which it obtains information, nor what type of information it collects or how it tracks the Internet to collect data.

The privacy policy of the Brazilian start-up Social Miner mentions that the company uses data from third parties such as Google and Facebook while providing data to these companies. This exchange of information reveals a situation familiar to most CDDBMs: their business

relationship (back and forth) with Google, Amazon, Facebook, Apple, and/or Microsoft. In this specific case, Social Miner allows connecting via Facebook, which gives the start-up sign-in information on the platform and in exchange provides the social media site with Social Miner's browsing information. In other words, it is a partnership in which both companies take advantage of the data, while the user increases his or her comfort and/or ease of connection.

The Matryoshka Doll: Home Buttons and Pages on Social Media Sites.

There are at least two sides to the relationship between CDDBMs and GAFAM. First, several companies use sign-in buttons or interoperability tools to exchange data on their websites or mobile applications. Second, smaller CDDBMs have social media pages to advertise their products and attract new customers or use Google Analytics services to measure the performance of their applications and their interrelation with their users/customers. For example, in Chile, AIRA, Falabella, and PedidosYa have Facebook pages, through which they share advertisements and strengthen the bond with their followers. This allows Facebook to collect additional information from the application's users, while offering its platform to disseminate its content and reach more people. In the Brazilian case, iFood states that it might share data with its partners to develop more assertive marketing campaigns, stating that it will "share the data only with those who have a privacy policy offering protection levels similar to those offered" by their policy. Furthermore, third parties conducting marketing activities in iFood's application or website, that is, which promote the advertisement of third-party products in such spaces, "may use cookies or other proprietary technology in iFood services, such as Facebook, Google Analytics and Double Click" to evaluate the performance of the marketing campaigns. A similar situation happens with the Brazilian company Social Miner. In this case, every time a user browses the company's website, the visit is transformed into data processed by Google Analytics.

It seems that vagueness is characteristic of these data exchange between companies, especially when the relevant product is the result of a partnership between two companies or when a single company owns two different products. The first scenario is the case of Amazon Prime Video in Brazil, which is a product of Amazon.com Inc., but is offered through the telephone operator Vivo. Although a user in Brazil may access Amazon

Prime Video's terms of service, these are not available in Portuguese, do not clearly establish whether the data collected by Vivo is considered as third-party data nor the relationship between both companies on the subject. The second scenario (two products, one owner), is the case of Facebook, which simultaneously owns Facebook, Instagram, and WhatsApp. Although the privacy policies of the latter in Colombia mention that, when sharing information with third parties—even with the members of the Facebook corporate group—WhatsApp requires them to comply with its conditions. What happens in the opposite case is not clear.

Facebook's data use policy is a particular case regarding its relationship with other applications. As an example of the interoperability between Facebook and other companies, the former informs that the partners "provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see," and more.[199] In any case, this is not the only reference to data "behaviour" in Facebook's privacy policies. This time, however, data flows the opposite way. According to the information provided by this social media site, "when you choose to use third-party apps, websites, or other services that use or are integrated with, our Products, they can receive information about what you post or share." Similarly, "apps and websites you use may receive your list of Facebook friends."[200]

1.2. Processing

In absolute terms, the processing of personal data includes practically any activity related to personal data. This includes, among others, data collection, assignment, transfer, and transmission activities, regardless of the method and the circumstances of time, means, and place of those involved in these activities. Some of this is presented above in the section on web tracking practices, the use of cookies, and other—more subtle—forms of sharing information. In this section, we will briefly focus on the CDDBMs' data processing practices related to information analysis.

The analysis and classification of personal information as a form of processing are typical to several CDDBMs. These forms of processing

---

199. This explanation is available in the section "Information from partners" of Facebook's privacy policy at https://es-es.facebook.com/privacy/explanation

200. For more information, see the section "Apps, websites, and third-party integrations on or using our Products" of Facebook's privacy policies at https://es-es.facebook.com/privacy/explanation

have the purpose of creating information solutions with an added value, for example, by identifying consumption patterns and users' preferences. These assets are useful for improving users' experience, building customer loyalty, and optimizing the marketing and advertisement activities and strategies of third-party products and services.

The results of the analysis and personal data processing may be descriptive or prescriptive. These are descriptive when performed to segment or profile users according to a categorization of personal data based on individual interests, tastes, or habits. These are prescriptive when their goal is to predict or induce the behaviour of the data subject. In general, the privacy policies of the CDDBMs do not indicate the technologies or big data methods used for this type of processing.

None of the companies analyzed in Mexico refer to this issue. In Chile, Facebook and Falabella simply indicate that they analyze data to segment their users and personalize content, but do not mention how they perform this analysis. The privacy policies of some of the CDDBMs studied in Colombia and Brazil have a higher level of detail, although not the desirable one. Microsoft, Netflix, Google, Social Miner, and AliExpress mention that they use automated processes, machine learning, algorithms, or Google Analytics to analyze data. It is worth noting that such concepts are extremely vague and indeterminate. Although it is an improvement compared with those companies that omit information on this subject, indicating the use of automatic systems, algorithms, or machine learning does not allow ordinary people—or even experts—to know what happens with their data and how it is being processed.

The lack of transparency or specificity of the privacy policies studied, concerning the methods by which the CDDBMs analyze personal data, is compounded by the legal silence on the subject. None of the countries studied oblige the data controllers to indicate the technology used to process information. A clarification of the regulations on this matter is of the utmost importance: it would allow users to get an idea of what happens to their personal data once it has been handed over or collected and would safeguard the aspiration of free and informed consent, which ultimately legitimizes any processing of personal data in the private sector.

1.3. Purposes of Personal Data Processing

The processing of personal data by CDDBMs analyzed here generally pursues two objectives. First, to provide the service, and hence improve the

user's/customer's experience, offer new products or services, and conduct market research. Second, sharing this information or the products of this information with third parties.

In most cases, the privacy policies studied are reasonably clear regarding the purposes of their data processing. In this line, the privacy policies of Falabella (Chile), Telcel (Mexico), and Magazine Luiza (Brazil) include easy-to-understand listings regarding processing purposes in their privacy policies. Mexico's Telcel and Payclip mention that there are primary purposes—essential to provide the service—and secondary purposes—those from which the user may opt out and, therefore, exclude their data from processing. The primary purposes coincide with the purpose of the CDDBMs. Consequently, they are necessary to provide the service or execute the platform's function (providing the telephone service, enabling invoicing, arranging for delivery of the product to the customer's home, etc.). Secondary purposes are related to communications with the client to expand the service or execute new contracts (send advertisements, reports on the company, assignment to third parties for specific purposes, etc.).

However, not all CDDBMs meet these transparency standards. In Chile, AIRA merely indicates that it will only use the information collected concerning the services provided. Amazon, on the other hand, suggests in an illustrative, but not exhaustive way, some of the purposes for which it processes data, leaving the door open for more to exist. The lack of clarity also stems from the difficulty a user may have in finding the information. Facebook's case is noteworthy, as it does not have a single list of purposes. Still, these are scattered throughout the entire privacy policy, depending on the subject addressed in each section. This practice prevents users from easily getting the information they need about the purposes for which Facebook uses their data.

2. Data Protection Laws in Brazil, Chile, Colombia, and Mexico

The analysis of legislation on data protection determines the preparedness of a legal regime to face the challenges of the digital age. According to the conclusions of the reports on the four countries studied, local legislation is not sufficient to regulate the data collection and processing dynamics of CDDBMs. In this section, we will present the common aspects that

condition the preparedness of the regulations in Brazil, Chile, Colombia, and Mexico to face the typical data processing practices of the digital economy. For this, we will focus on three aspects: 1) the scope of application of the national law, 2) the (in)adequacy of the legislation to deal with phenomena of the digital age, and 3) the capacities/competences of the data protection authority.

2.1. Scope of Application of the Law

Following the general principle of law on the territorial application of laws, data protection legislation in Chile, Colombia, and Mexico apply almost exclusively when data is processed in the country and by data controllers domiciled within the national territory.[201] However, the Mexican law includes an additional assumption: when the controller "is not constituted in Mexican territory and uses means located therein, except when said means are used solely for traffic that does not imply processing." In Colombia, Article 2 of Law 1581 of 2012 provides that the regulation shall also apply to "controllers not constituted in the national territory, but the Colombian legislation is applicable under international norms or treaties."

2.1.1. The Domicile of the CDDBM as a Criterion for the Territorial Application of the Law

The laws of Chile, Colombia, and Mexico apply, in principle, to data controllers domiciled within the State's territorial jurisdiction. This derives both from a literal interpretation of the legal text—or rather from its silence on the matter—and, in part, from judicial practice. In Mexico, the INAI has interpreted that the data protection legislation does not apply to persons domiciled in other countries. This situation reflects one of the most significant challenges of regulating these issues in Latin America. Since the standard for applying the law is the place where the processing is performed or where the processor is domiciled, local laws would not apply to large Internet companies such as Google, Apple, Facebook, Amazon, or Microsoft. These companies are generally domiciled in the United States, and have offices around the world—it is not clear if these are affiliates.

---

201. According to Article 2 of Law 1581 of 2012 (Colombia) and Article 4 of the LFPDPPP regulations (Mexico), the national regulation shall apply when the processing takes place in the territory or when the data controller is not domiciled in the national territory, but the country's laws apply to it under international conventions or treaties.

Since 2019, the Colombian data protection authority has considered that the Colombian law applies to transnational companies collecting data from people living in the national territory, considering that the collection is part of the processing and, thus, it is conceivable that the processing is performed within the State's territory. In furtherance of this interpretation, this authority has issued resolutions instructing Facebook and Uber, two companies not domiciled in Colombia, to protect the personal data of Colombians.[202]

In Chile, Law N° 19.628 does not refer to its scope of application. In practice, this has led to its interpretation being limited, in compliance with the general principles of law. For this reason, although there is no express provision on the matter, Law N° 19.628 is applicable only to the processing of personal data performed in Chilean territory. Strangely, the bill being discussed in the Chilean Congress does not contain special provisions on the territorial application of the law, a critical aspect concerning the processing practices and actors in the digital era. At most, this project requires that the controller who is not domiciled in the territory, but processes data of nationals, has a contact mailbox with an email address for this purpose.

2.1.2. The Domicile of the Data Subject as a Requirement for the Territorial Application of the Law

From the effective date of the European Union General Data Protection Regulation (GDPR), the territorial scope of application of the European data protection regulation no longer depends on the domicile of the controller, but the domicile of the subject whose data is being processed. According to Article 3 of the GDPR, the regulation applies:

> To the processing of personal data of subjects residing in the Union by a controller or a processor not established in the Union, when the processing activities are related to: the offer of goods or services to said subjects in the Union [...] or to the monitoring of their behaviour.

---

202. In this regard, see Resolution 1321 of 2019 (Facebook case) and Resolution 21478 of 2019 (Uber case) issued by the Deputy Superintendence for the Protection of Personal Data of the Superintendence of Industry and Trade. Both decisions were appealed. However, in the Facebook case, the second instance decision confirmed the first instance decision. In Uber case, the second instance had not been resolved as of the publication of this document.

This means that transnational companies like GAFAM must comply with the European regulations—even if they are not domiciled in Europe—provided the processing of personal data is roughly related to situations typical of the digital economy.

Inspired by the GDPR, Article 3 of Brazil's Law 13.709 of 2018 provides that the national regulation applies in the following scenarios: 1) when the processing is performed in Brazil, 2) when the processing's purpose is to offer goods and services, and 3) when the personal data being processed are collected within the national territory—that is, when the data subject is in Brazil. The Brazilian law will become effective in mid-2020; therefore, as of the date of completion of this report, there are no data that indicate its effectiveness.

The recent interpretation by the Colombian data protection authority on the scope of application of the law is quite similar to the provisions of the GDPR and the Brazilian regulation. According to this authority, transnational companies must comply with the Colombian law because they process (i.e., collect) personal data in Colombia. It is worth noting that Facebook and Uber appealed these decisions, as they considered that the Colombian data protection law does not apply to them. As of the completion of this report, the Colombian data protection authority, an administrative body, had confirmed the sanctioning decision against Facebook in the second instance.

2.2. Inadequate or Insufficient Regulation for the Digital Age

Out of the regulations of the countries studied, the one most in line with the new practices and technical developments of the digital age is the Brazilian legislation (Law 13.709 of 2018). The legislation of the other countries analyzed (Chile 1999, Mexico 2010, Colombia 2012) are indifferent—in the best-case scenario, following the principle of technologic neutrality—to the language and specificities of the 21st century digital practices. Although their general and abstract terms allow a gradual interpretative adaptation to the sophisticated practices of personal data processing typical of the digital economy, the studies mentioned in this book show the convenience of adapting such regulations or of adapting their interpretation to face, among others, problems related to web tracking, identification of personal data by accumulation and linking (inferred personal data), profiling, predictive analytics, automated decision-making, the right to effective access to personal information, and the right to oppose processing, among others.

2.2.1. Web Tracking, IP, and the Definition of "Personal Data"

One of the elements common to the legislations of Brazil, Chile, Colombia, and Mexico is that there is no clarity on the legal status of the data collected through monitoring or web tracking. This is problematic because, as we have seen (e.g., in the cases of the Brazilian companies iFood and Social Miner), CDDBMs consider that the information they obtain through this practice does not constitute personal information—e.g., it would be statistical information—and, consequently, consider that the data protection legislation does not apply to them.

The definition of personal data under the legislation of the countries studied is maximalist and uses positive universals[203] which undoubtedly facilitate interpretative adjustments. However, given the sophistication of data collection practices in highly technical contexts, the following questions are relevant: Does the information on the device, the browser used, and the search history from the device constitute personal data? Is a device's Internet Protocol (IP) information—which allows identifying any device and the place in the world from which the device connected to the Internet—personal data? Is this regardless of whether different people use such devices or appliances?

The legislation of the countries studied does not contain any explicit provision that considers online identifiers or the interactions between devices and platforms as personal data. These are the essential elements of Internet interactions and are fundamental to the operations of CDDBMs. To avoid this legal uncertainty, legislators in Europe and California chose to include information that can be collected through web tracking, and that is usually related to our devices, within the definition of personal data.[204] This eliminates the possibility that the collection and processing of

---

203. According to Article 3(c) of Law 1581 of 2012, in Colombia, personal data is information "linked or capable of being linked to one or more specific or ascertainable natural persons." In Chile, Article 2(f) of Law N° 19.628 provides that personal data are those "relative to any information on identified or identifiable natural persons." Similarly, the Mexican legislation defines personal data as "information relating to an identified or identifiable person" (LFPDPPP, Article 3[V]). In turn, Brazil's General Data Protection Law defines personal data as the "information regarding an identified or identifiable natural person."

204. In this sense, the Section 1798.140 of the CCPA provides that the concept of personal information includes, but is not limited to, the Internet Protocol (IP) address, email address, geolocation data, Internet activity, browsing history and any other customer's interaction with an Internet Website or

this information by CDDBMs takes place without any possibility of control. It also shows how personal data protection regulations can best fulfill their function if they are adjusted to the requirements of the digital age and recognize that the dynamics of the digital economy include the large-scale exploitation of data collected through online interactions.

2.2.2. Cookies and Transparency

Just like with other technological tools that facilitate collecting information, the laws of Brazil, Chile, Colombia, and Mexico do not refer to the use of cookies or other web-tracking technology. Nor do they regulate how clear and understandable the information should be. Is it enough—and understandable for the average user—to mention that the application or website uses cookies to collect information? Would it not be advisable to include sub-rules on cookies at the legal or interpretative level in the context of the obligations of transparency, finality, and purpose? These questions become more relevant when it comes to the collection of sensitive data. For example, in Chile, personal habits, which include a person's Internet activity, are considered sensitive data and, therefore, enjoy a higher degree of protection. However, the technical inadequacy of data protection regulations in the digital age dilutes the possibility of greater controls on the use of cookies. Not even the Brazilian legislation issued in 2018 has specific provisions on this matter, which is surprising.

2.2.3. Inferred Sensitive Data

The legal regimes studied face the challenge of regulating the processing (storage-collection-identification) of inferred data, particularly of sensitive inferred data and data used to infer such data. Thanks to the development of data mining techniques and big data analysis, CDDBMs can infer data about people without them giving it directly and voluntarily. These practices enable specifying and making explicit new information which, once "produced," can be considered as sensitive data.

There is relative agreement on the prohibition, with some exceptions, to processing sensitive data, and on the particular duties of safeguarding

---

mobile application. In contrast, Recital 30 of the GDPR recognizes that "natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols." Thus, when defining the concept of personal data as all information related to an identified or identifiable natural person, it mentions that "an identifiable natural person is one who can be identified [...] in particular [...] location data, [or] an online identifier" (GDPR, Article 4[1]).

and processing this specific type of personal information. However, this prohibition and these duties are inapplicable in practice because CDDBMs acquire the information—or come quite close to it—through data inferring. Sensitive data (sex/gender, sexual orientation, political views, health status, religious beliefs, etc.) can be inferred by analyzing non-sensitive data sets (e.g., search history, purchases, etc.). What becomes apparent from this study is that several CDDBMs effectively process these data in ostensible anomie. This is because there is no legal provision regulating the collection and processing of sensitive data through data analytics or data inference or matching processes.

2.2.4. Profiling

Another aspect not regulated by the legislation studied is the creation of profiles (or profiling) of users for any purpose, with automated decision-making (for marketing purposes) being the most common use. Automated profiling is possible thanks to big data, data crossing, and data mining. Thus, a large amount of information is analyzed and systematized to identify each person by employing different and numerous information units (data points) that, when massively collected, related, and put into context, can say something (or a lot) about a person. This situation is significant. CDDBMs often use the virtual profiles of a physical person to determine the services to which it has access and the products it may acquire, or to affect his or her rights, the information provided to him or her, and the decision of whether or not to be placed under active surveillance (Büchi et al. 2019).

Although CDDBMs in general profile their users for commercial purposes, such as offering targeted advertising and providing access to certain goods or services, this corporate practice is not exempt from risks, especially those associated with modifying people's online behaviour (Marder et al. 2016). Some authors claim that users change their browsing habits by trying to anticipate automated decisions resulting from profiling (Gräf 2017), which poses unexplored risks to individual autonomy (Kandias et al. 2016). The lack of regulation on how profiling can be done, or on automated decisions based on it, leaves users at a total disadvantage vis-à-vis the power of action and decision of CDDBMs.

2.2.5. Regulatory Response to Profiling

Considering the above risks, the European GDPR establishes the obligation to inform users when they will be subject to automated decisions and

profiling. This obligation includes the duty of informing on the logic involved—that is, how the system works—and its possible consequences for people (Article 61). This regulation also indicates that individuals may object to the processing of personal data when it involves profiling or automated decision-making that significantly affects them (Article 21(1)). It is important to note that the bill being discussed in the Chilean Congress reflects some of these lessons and includes a definition of profiling. The laws of Brazil, Colombia, and Mexico are silent on this matter, which leaves the data subject without specific protection.

2.2.6. The Right to Object

The right to object entitles the data subject to regain control over his/her personal information and inhibit processing activities if they are illegal or illegitimate. However, the non-existence of this right in the Chilean and Colombian regulations, and its proven ineffectiveness in Mexico, is another regulatory (or interpretative) gap identified in this study. For example, all the privacy policies analyzed in Colombia must be accepted or rejected en bloc, without allowing a person to object to the processing of personal data in a certain way or for a particular purpose, either from the start or during the phases following the processing. Similarly, the Mexican law does not provide mechanisms to exclude the authorization of data use, automated decision-making, or profiling. This right (also known as the right to opt out) would give users greater control over their personal data. It is not in vain that the European regulations and the CCPA—concerning the marketing of data (Section 1798.120)—allow users to object the processing of personal data in a certain way and partially give their consent.

2.3. Capacities of the Data Protection Authority

Not all legal systems provide for the existence of a personal data protection authority. However, Brazil, Colombia, and Mexico have a national data protection authority, and the process for its creation is underway in Chile. This seems to reflect the importance of a personal data protection authority to safeguard the fundamental rights of individuals in the context of massive and intensive data processing.

2.3.1. The Extent of Competence and the Territoriality Problem

The competence of the data protection authorities depends on the scope of application of the data protection regulation to a large extent. In Chile,

Colombia, and Mexico, the law does not seem to recognize its competence to perform control and monitoring activities over the CDDBMs not domiciled in the country or which process personal data in another country. As seen, this could mean that, in principle, the data protection authority has no competence to rule upon the data processing performed by companies such as Facebook or Google, even if the data belong to Colombian or Mexican nationals.

However, in 2015, the Mexican data protection authority issued a resolution against Google on a case related to the right to object of a Mexican data subject. This decision was subsequently revoked at court, and the case is still ongoing. For its part, in 2019, the Colombian data protection authority sought—by interpretation—to extend its monitoring and control powers to cover CDDBMs domiciled in other countries but collecting data in the national territory; however, these criteria have not yet surpassed the judicial review.

Despite these valuable interpretative efforts, strengthening the capacities of these authorities depends, among other things, on all institutional actors adequately and comprehensively interpreting the regulation's scope of application. This would clarify the competence of the data protection authority concerning the CDDBMs processing personal data of nationals of the respective State. In this sense, an explicit modification to the laws or a comprehensive interpretation that conforms to the digital reality is advisable. A potential regulatory alternative may be that adopted by the Ibero-American Standards (Recital 22), the GDPR, and the Brazilian regulations, whose determining factor is the residence of the data subject. This can be achieved by amending local legislation, through broad interpretations of the existing norm or, ideally, by adopting a regional and international treaty on the matter.

2.3.2. Institutional Capacities

Beyond the difficulty of holding transnational companies accountable, the capacity of the data protection authorities to respond to the dynamics of the digital age is limited. This is for two reasons. First, because safeguarding this right requires those working at the data protection authority to have extensive knowledge in two complementary areas: 1) computer sciences, that is, basic knowledge on how the Internet, data marketing, machine learning, artificial intelligence, big data, and algorithms work,

among others; and 2) legal sciences, especially regarding electronic commerce, intellectual property, right to data protection, and human rights in the digital age.

Second, the procedural requirements for triggering rulings, various barriers to entry, and the absence of staff or qualified personnel prevent the authority from efficiently performing its duties. Both the INAI in Mexico and the Deputy Superintendence for the Protection of Personal Data in Colombia have had meager results in addressing and solving requests and/or complaints by data subjects. For instance, in Mexico, there were only 251 requests for Rights Protection Procedures before the INAI (in which a CDDBM was not necessarily involved) in 2018. Of these, less than 25 resulted in the modification and/or settlement of the situation. This figure is indicative of the remarkably low number of requests submitted to the INAI in comparison to Mexico's population (approximately 120 million people) and is also indicative of the relatively low success ratio of the procedure.

In contrast, in Colombia, the Deputy Superintendence for the Protection of Personal Data of the SIC receives a high number of claims every year. According to statistics available on its website, in 2016 there were 2,230 personal data protection complaints being processed. In the same year, the Deputy Superintendence issued almost 400 orders or fines to remedy rights violations. However, the number of incoming processes is much higher than the capacity to solve them, which leads to long wait times.[205] As a result, the number of officials working at the data protection authority has increased since 2018, which may increase its effectiveness. In this sense, according to the entity, nearly 1,000 orders or fines were imposed, and three guidelines on current issues (electronic commerce, international data transfers, and marketing and advertisement) were published in 2019. This shows a substantial improvement in the capacities of the Deputy Superintendence for the Protection of Personal Data.

2.3.3. Institutional Design

The institutional design of the data protection authority is a significant issue, particularly when it seeks to enhance its independence from public and private powers.

---

205. 2015 process indicators on Administrative Personal Data Protection Monitoring. Statistical Data-Institutional Management, breaking down the activities of the SIC from 2013 to 2016.

In Mexico, the technical and budgetary autonomy of the INAI is apparent, and its independent nature is stated in its description as an autonomous state entity and its composition of seven commissioners appointed by the Senate of the Republic. The cases of Colombia and Brazil contrast to what could be considered an adequate institutional design.

Although the data protection authority has specific technical and budgetary autonomy in Colombia, the entity is a delegate of the President of the Republic. The Deputy Superintendence for the Protection of Personal Data is a department within the Superintendence of Industry and Trade, the State office that monitors and inspects the industrial and commercial activities performed in the country.

The case of Brazil is similar. The *Autoridade Nacional Proteção de Dados Pessoais* is attached to the Civil House of the Presidency of the Republic. Within this institutional structure, the authority is ascribed to and subject to the will of the Executive Branch. The presidency was against the Congress being the body in charge of legislating on the matter, as it considered that it was a matter of exclusive competence of the presidency because it was related to the organization of the public administration. Therefore, the Brazilian data protection authority has no budgetary autonomy or full freedom to trace its agenda, an unfortunate institutional arrangement in adequately safeguarding individuals' right to data protection.

Finally, we are uncertain about the outcome of the creation of the Chilean data protection agency and whether it will be independent of other political powers. It is worth mentioning that the definition of the nature and place of this authority in the Chilean institutional context is the result of a power struggle between the Executive and the Legislative. In August 2019, the Senate confirmed that it would accept the Executive's proposal, according to which the Transparency Council would be transformed into the new national data protection authority. Although this Council has enjoyed a certain degree of autonomy so far, whether this will continue being the case is uncertain, mainly because of budgetary and institutional capacity issues.

Conclusions and Recommendations

The CDDBMs analyzed in Brazil, Chile, Colombia, and Mexico collect and process personal data in the context of the digital age and through special and ever-changing technological tools. The diversity of business

strategies and corporate purposes of the CDDBMs is reflected in their privacy policies. These, in turn, express the concept of business and corporate values concerning personal data collection and processing practices. Generally speaking, the CDDBMs studied try to adjust their practices to local legislation.

However, the particular position of GAFAM and their dual nature as Internet giants and foreign companies (all with main domicile in the United States) reveals certain conundrums about the adequacy of personal data collection and processing practices and the terms and requirements of local laws. This situation is compounded with the versatility of collection and processing practices in a particularly changing scenario and the constant novelty of the available technologies. These range from sophisticated web tracking practices to the refinement of data analysis tools in a scenario of massive data concentration and tremendous personal information storage and processing capabilities.

The studies analyzed here also reveal the growing role of GAFAM in the digital economy environment. For obvious temporary reasons, they also reveal that the state legislation, especially that of Chile, Colombia, and Mexico, is outdated or its current interpretation is insufficient. Although on occasions the studies recognize the possibility of adapting or interpreting the current provisions to regulate these "new" practices, they also indicate the relevance—or the need—to adapt the legislation to deal with these new situations and thus be able to fulfill the promise of enforcing the fundamental right to data protection in the digital age.

The comparative exercise of the studies compiled here has revealed at least three major types of issues in terms of the collection and processing practices of CDDBMs in the digital age. The first relates to transparency and consent. The second is related to the need to adapt the legislation to the specific practices of the technologies that support the CDDBMs' business scheme. Moreover, the third problem is related to safeguarding the fundamental right to the protection of personal data.

The problem of transparency is pressing. Personal data collection and processing practices are highly sophisticated. The collection takes place in various ways and not only directly from the source through more or less clear registration processes. Web tracking and the use of different mechanisms to share information, such as social media buttons, especially Facebook or Google Analytics, are not sufficiently clear or explicit. The privacy policies that describe in detail the type of personal data collected,

or explain the complex interactions between different agents that, in one way or another, end up in possession of the personal data of the nationals of the States under study, are rare. The demand for transparency is confronted with the fact that the information relating to the processing contained in these privacy policies is in a highly technical language, is scattered in several documents, is only available in a language that is not the official language of the country where the collection of the personal data takes place, or is contained in flat and extensive texts. All this is to the detriment of a basic idea: that ordinary people understand or can understand which data is collected, for what purpose it will be processed, and the effects, implications, and duration of the collection.

The problems related to a lack of specific regulation that addresses the technical complexity of the collection and processing practices deserve special attention by relevant actors (legislators, national data protection authorities, academics, stakeholders, and activists). At the least, web tracking practices, the intensive use of different types of cookies, the possibility of identifying data through inference or relation, profiling practices with different purposes, the use of various data relation, analytics, and mining tools, and the use of complex algorithms should be explicitly regulated and, from there, also the sophistication of digital marketing, microtargeting, predictive analytics, and automated decision-making practices which may affect data subjects.

In this last hypothesis, consider, for example, the cases of displaying advertisements on certain products (apparently the most anodyne), even the most delicate ones such as the construction of information bubbles, or explicit or subliminal induction for individual decision-making. The studies analyzed here show the limitations of the legislation on fundamental issues, including the definition of the nature of the IP address as personal data, the existence of different cookies, and the need for data subjects to have control over the type of personal information cookies can collect, or the need to protect people's freedoms in the face of growing automated decisions.

Finally, the studies also reveal that the safeguards to the right to data protection in the digital age are insufficient, and the critical context of the operation of the CDDBMs and their relationship with GAFAM. Not only because of the problem of extraterritorial application of local laws—which is perhaps one of the biggest problems we face as a region—but also because of the problems related to the definition and scope of participation

rights in the collection and processing processes, and especially the scope of the right to object. That is, the right of the data subject to claim ownership of the data and to object to the processing of his or her personal data once it is found to be illegal or illegitimate.

However, although this right is recognized and affirmed as such by local legislation, the institutional conditions to safeguard it are lacking: effective and speedy judicial processes, such as the *amparo,* are not the rule in the regulations studied, and the institutional capacities of the personal data protection authorities have been called into question. In some cases, due to the difficulties in articulating the administrative procedures and the limitations inherent to the internal legal regimes (Mexico, Colombia); in others, because the fines are not sufficiently dissuasive (Chile), and in others, due to the lack of independence or political will (Brazil) and, in general, due to the precarious technical and operational capacities, and to the manifest power imbalance between the data protection authorities and the controllers (GAFAM).

Problems of adequate transparency, regulatory deficiencies, and the absence of sufficient safeguards are bad news for the data subject in the digital age. This diagnosis aggravates the unequal power relationship between data subjects and CDDBMs, and especially between the former and GAFAM. Also, not all national laws (or the dominant interpretation in each country) apply to transnational companies processing personal data such as Google or Facebook.

Based on these conclusions, we make the following recommendations, inspired by the dual purpose of balancing the power relationship between CDDBMs and data subjects, and of advancing the agenda of safeguarding—and hopefully enforcing—the fundamental right to data protection for digital users:

- Establish the principle of transparency as a guide for privacy policies (or terms of service) to inform how and for what purposes companies collect and process personal data. Especially, regarding 1) any assignment of data between applications or CDDBMs; 2) the commercial and/or collaboration relationship between applications and GAFAM; 3) the profiling of users for commercial or advertising purposes; and 4) automated decision-making based on these profiles or the activities of data subjects.
- Adapt local legislation or their interpretation to the digital environment. Especially, regarding 1) the collection of data through

web tracking, cookies, and other digital tools; 2) the inclusion of device-related information, such as the IP address, the browsing and search history, and geolocation, within the concept of "personal data."

- Adequately acknowledge (as the right to habeas data) the data subjects' right to object to certain types of processing and specific subjects (marketing of data, automated decisions, profiling, etc.), without conditioning the provision of the service.
- In countries where this is not yet the case, extend the scope of the national legislation to cover the processing of personal data by companies not domiciled in the country, while explicitly recognizing the competence of local data protection authorities. On this point, the proposal of the Ibero-American Standards, the GDPR, and the Brazilian legislation or Colombian data protection authority to consider the place of residence of the data subject or the place of collection of the data as criteria to apply the personal data protection legislation, is acceptable.
- Strengthen the technological and legal capacities, the independence from the Executive power, and the investigation and sanctioning powers of each State's personal data protection authorities.
- Promote and strengthen the work of the Ibero-American Data Protection Network as a meeting place for the region's data protection authorities.
- Adjust national legislation to regulate data protection, based on minimum protection standards. This is so that the transnational companies can adapt to the market of the four countries without the risk of fragmentation and increase the bargaining power of the region's countries vis-à-vis the transnational CDDBMs. This could be achieved by further developing the minimum agreements reached in the "Standards for Data Protection for the Ibero-American States" created by the Ibero-American Data Protection Network.[206]

206. 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

- Based on the previous minimum requirements—duly incorporated into local legislation—promote the creation of a regional regulation common to the Latin American States and adjusted to the dynamics of the digital age. This regulation should also allow the promise of an efficient fundamental right to the protection of personal data of the nationals of these States and to confront, as a region, the power of the transnational CDDBMs.

References

Büchi, Moritz, Eduard Fosch, Christoph Lutz, Aurelia Tamò-Larrieux, Shruthi Velidi, and Salome Viljoen. 2019. "Chilling Effects of Profiling Activities: Mapping the Issues." SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379275

Gräf, Eike. 2017. "When Automated Profiling Threatens Our Freedom: A Neo-Republican Perspective." *European Data Protection Law Review* 3, no. 4: 441–451.

Kandias, Miltiadis, Lilian Mitrou, Vasilis Stavrou, and Dimistris Gritzalis. 2016. "Profiling Online Social Networks Users: An Omniopticon Tool." *International Journal of Social Networks Mining 2*, no. 4: 293–313.

Marder, Ben, Adam Joinson, Avi Shankar, and David Houghton. 2016. "The Extended 'Chilling' Effect of Facebook: The Cold Reality of Ubiquitous Social Networking." *Computers in Human Behavior 60*: 582–592.

ABOUT THE AUTHORS

Kimberly Anastácio holds a Bachelor's degree and a Master's degree in Political Science from the Universidade de Brasília. She was a researcher at the Department of Public Policy, Fundação Getulio Vargas, and is a data coordinator at Isobar. She collaborates with Coding Rights on human rights and Internet issues.

María Paula Ángel-Arango is a lawyer awarded with the *Cum Laude* distinction and a political scientist at the Universidad de los Andes. Her Master's degree in Administrative Law is from the Universidad del Rosario. In 2019, she received the Fullbright-Colciencias scholarship for her PhD studies. She is currently studying for her PhD in Law at the University of Washington, Seattle, and is a research assistant at their Tech Policy Lab.

Paloma Herrera Carpintero is a lawyer with a Bachelor's degree in Legal and Social Sciences from the Universidad de Chile. She has also completed a Diploma course in Cybersecurity at the Universidad de Chile. She is a Collaborator at the Center for Studies in Information Technologies Law, Universidad de Chile.

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 postgraduate 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.

Bruna Martins dos Santos is a lawyer who studied at the Centro Universitário de Brasília. She is also an analyst at Coding Rights, Coordinator of Internet Governance Caucus, and member of the Non-Commercial Users Constituency at Corporação da Internet para Atribuição de Nomes e Números.

Milan Trnka Osorio obtained his law degree from the Universidad Nacional Autónoma de México (UNAM). He is the legal officer at R3D: Red en Defensa de los Derechos Digitales.

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.

Joana Varon is the executive director of Coding Rights and is a Mozilla Foundation fellow. She is also affiliated with the Berkman Klein Center for Internet and Society at Harvard University and a member of the Open Technology Fund Advisory Council.

Pablo Viollier Bonvin is a lawyer who holds a Bachelor's degree in Legal and Social Sciences and Diploma course in Cybersecurity from the Universidad de Chile. He currently works as a Digital Rights Public Policy Analyst and is a professor at Universidad Diego Portales.

WORKING PAPER

• WORKING PAPER 1

ADDICTED TO PUNISHMENT
The Disproportionality of Drug Laws in Latin America
Rodrigo Uprimny Yepes, Diana Esther Guzmán & Jorge Parra Norato
available in paperback and in PDF from www.dejusticia.org
2013

• WORKING PAPER 2

MAKING SOCIAL RIGHTS REAL
Implementation Strategies for Courts, Decision Makers and Civil Society
César Rodríguez-Garavito & Celeste Kauffman
available in PDF from www.dejusticia.org
2014

• WORKING PAPER 3

COMMUNICATIONS SURVEILLANCE IN COLOMBIA
The Chasm between Technological Capacity and the Legal Framework
Carlos Cortés Castillo & Celeste Kauffman (trans.)
available in paperback and in PDF from www.dejusticia.org
2015

• WORKING PAPER 4

VICTIMS AND PRESS AFTER THE WAR
Tensions between Privacy, Historical Truth and Freedom of Expression
Vivian Newman, María Paula Ángel & María Ximena Dávila
available in PDF from www.dejusticia.org
2018

• WORKING PAPER 5

PALLIATIVE CARE
A Human Rights Approach to Health Care
Isabel Pereira Arana
available in PDF from www.dejusticia.org
2018

• WORKING PAPER 6

FRAUGHT WITH PAIN
Access to Palliative Care and Treatment for Heroin Use Disorder in Colombia
Isabel Pereira Arana & Lucía Ramírez Bolívar
available in PDF from www.dejusticia.org
2019

DEJUSTICIA WORKING PAPER SERIES

• WORKING PAPER 7

ACCOUNTABILITY OF GOOGLE AND OTHER BUSINESSES IN COLOMBIA
Personal Data Protection in the Digital Age
Vivian Newman-Pont & María Paula Ángel Arango
available in PDF from www.dejusticia.org
2019

• WORKING PAPER 8

SARAYAKU BEFORE THE INTER-AMERICAN HUMAN RIGHTS SYSTEM
Justice for the People of the Zenith and Their Living Forest
Mario Melo
available in paperback and PDF from www.dejusticia.org
2019

• WORKING PAPER 9

NEGOTIATING FROM THE MARGINS
Women's Participation in Colombian Peace Processes (1982–2016)
Nina Chaparro González
Margarita Martínez Osorio
available in paperback and PDF from www.dejusticia.org
2020

During a conversation with Mark Zuckerberg

in April 2019, Israeli historian and philosopher Yuval Noah Harari wondered about the dangers of remote computer systems that know us better than our mothers, and whose interests are not necessarily aligned with ours. The accumulation of information on a massive scale, he says, has unleashed an unprecedented power in humanity's history. This power challenges the foundations of free will and freedom of choice for individuals, consumers, and citizens.

This book addresses the multiple challenges of this new type of system. It seeks to show how, in the digital age, companies pursue the massive collection of personal data and how they deal with their power of information accumulation while also trying to push forward their business strategy. In the case of the Internet giants—Google, Amazon, Facebook, Apple, and Microsoft (GAFAM)—they now possess an ability to reconfigure the behaviour of individuals, clients, and citizens globally.

Specifically, this book analyzes the privacy policies of selected companies that use data-driven business models in four Latin American countries: Brazil, Chile, Colombia, and Mexico. It also assesses how prepared these states are to protect their citizens against the exploitation of their personal data and to face the legal and technical challenges of Big Data in an ever-changing transnational context, and with actors more powerful than nation states.