Accountability of Google and other Businesses in Colombia:

Personal Data Protection in the Digital Age

Vivian Newman-Pont
María Paula Ángel-Arango

WORKING PAPER 7

Dejusticia
law · justice · society

Vivian Newman Pont

A lawyer from Universidad Javeriana and Bachelor of Laws from Universitat de Barcelona through homologation, Vivian holds a postgraduate in Administrative Law (D.S.U.) and two master's degrees (D.E.A.) in Internal Public Law from Université Paris II Panthéon-Assasand and in Cooperation and Development from Universitat de Barcelona. She is the author of *Datos personales en información pública: Oscuridad en lo privado y luz en lo público* (2015; *Personal data in public information: Darkness in the private and light in the public*) and currently works as the director of Dejusticia. Together, María and Vivian have co-authored three books: *Acceso a los archivos de inteligencia y contrainteligencia en el marco del posacuerdo* (2017; *Access to intelligence and counterintelligence archives in the post-agreement framework*), *Sobre la corrupción en Colombia: Marco conceptual, diagnóstico y propuestas de política* (2017; *On corruption in Colombia: Conceptual framework, diagnosis and policy proposals*), and *Víctimas y prensa después de la guerra: Tensiones entre intimidad, verdad histórica y libertad de expresión* (2018; *Victims and press after the war: Tensions between intimacy, historical truth and freedom of expression*).

María Paula Ángel Arango

A political scientist and cum laude lawyer from the Universidad de los Andes, with a master's degree in Administrative Law from Universidad del Rosario, María currently works as a researcher in Dejusticia's Transparency and Privacy area.

Accountability of Google and Other Businesses in Colombia

Personal Data Protection in the Digital Age

Vivian Newman Pont

María Paula Ángel Arango

Dejusticia
law · justice · society

Working Paper 7
ACCOUNTABILITY OF GOOGLE AND OTHER BUSINESSES IN COLOMBIA
Personal Data Protection in the Digital Age

Newman Pont, Vivian.
Accountability of Google and other Businesses In Colombia: Personal Data Protection in the Digital Age / Vivian Newman Pont, María Paula Ángel; translator Carlos Alberto Arenas. -- Bogotá : Dejusticia, 2019.
104 páginas : mapas y tablas ; 15 x 24 cm. -- (Working papers)
Título original : Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital.
ISBN 978-958-5597-00-6
1. Personal data protection 2. Google 3. Apple 4. Digital economy. 5. Big data. I. Ángel, María Paula, autora. II. Arenas, Carlos Alberto, traductor. III. Tít. IV. Serie.

ISBN 978-958-5597-00-6 printed version
ISBN 978-958-5597-01-3 digital version

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

Translation: Carlos Alberto Arenas
Copy editing: Ruth Bradley-St-Cyr
Cover photo: Sebastián Restrepo Calle
Layout: Diego Alberto Valencia
Cover design: Alejandro Ospina

Bogotá, October 2019

Contents

ACKNOWLEDGMENTS

Our research would have not been possible without the thematic and financial support of Privacy International, to which we express our gratitude. Additionally, the help and support we received from Alexandrine Pirlot de Corbion, Francisco Vega, and especially Ailidh Callander, were critical in enriching the contents of this document. Likewise, the feedback received from Juan Carlos Upegui greatly contributed to the successful development of this project.

We want to thank our friends and colleagues at Dejusticia who attended the focus group and took the time to read and comment on the first draft of this text. We also want to thank Carlos Cortés, José Alejandro Bermúdez, Daniel Castaño, Viviana Cañón, Juan Diego Castañeda, Grenfieth J. Sierra, Camilo de la Cruz, Lorena Lizarazo, Ana Carolina Molina, Celso Bessa, and Gabriela Hadid, who generously attended our focus group and enriched the contents of this document with their experience and opinions. Also, thanks to Laura Guerrero and Sophie Kushen, who made substantial contributions to the final changes to the text.

Lastly, thanks to the Dejusticia management team for their constant support in the performance of our daily tasks. Particularly, we want to thank Elvia Sáenz and Isabel de Brigard for their help and indispensable willingness throughout the editorial process.

INTRODUCTION

Hearing that data is the new oil is common nowadays.[1] What data are we talking about? We refer to the digital data constantly collected or generated by information and communication technologies (ICT), such as the Internet, social media, our mobile devices and apps, our public transportation smart card, or the sensors in our car engines and smart watches, just to name a few. And why is data the new oil? If digital data is properly refined and exploited, just like oil or any other high-value commodity, it generates economic and social value for both countries and companies.[2] How? By revealing patterns, correlations, and other information that would be impossible to know without data and data analytics.

Consequently, thousands of companies have been created around the world seeking to capture this value. Among them, Google, Apple, Facebook, Amazon, and Microsoft (hereinafter, GAFAM) excel due to their size and economic, technological, and social power, but there are also medium-sized companies and various digital startups. Likewise, several established companies have also begun to extract value from their data to optimize processes, improve their marketing strategies, or develop

1 Although this statement has been attributed to Clive Humby, an English mathematician and creator of the Tesco Clubcard, it has been repeated by several "technology capitalists." On the subject, refer to Haupt (2016).

2 According to the McKinsey Global Institute, "there is strong evidence that big data can play a significant economic role to the benefit not only of private commerce but also of national economies and their citizens. Our research finds that data can create significant value for the world economy, enhancing the productivity and competitiveness of companies and the public sector by creating substantial economic surplus for consumers" (Manyika, Chui, Brown, Bughin, Dobbs, & Roxburgh, 2011, pp. 1–2).

the quality and functionality of the goods and services they offer. This set of companies, which we will refer to as "companies with data-driven business models" (hereinafter, CDDBMs),[3] are revolutionizing the economy and have led to what we now call "the digital economy," which in turn influences politics and the rights of citizens.

The digital economy is rooted in "big data" (Corredor, 2015), defined 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, & Grimaldi, 2014, p. 8). Although not all big data corresponds to personal data, in fact "a large part of the information being generated today contains personal information. And companies have a large amount of incentives to capture more, maintain it for longer and reuse it more often" (Mayer-Schönberger & Cukier, 2013, p. 152). Furthermore, because of the large volume of data being generated nowadays, and because of the technological advances in processing that data (so-called "data analytics" or "Big Data processes"), the concept of personal data has been extended. In this way, "PII [Personal Identifying Information] is also about the amount of data; the more information someone has about you, including anonymous information, the easier it is for them to identify you" (Schneir, 2015, p. 53).

Thus, the development of the digital economy and big data pose significant challenges for the rights to privacy,[4] the protection of personal data,[5] and equality, as well as for transparency and data security. On this

---

3 Although this concept generally refers to companies with "business models that rely on data as a *key resource*" (Hartmann, Zaki, Feldmann, & Hartmann, 2014, p. 6; italics added), there are several data-driven business models that use and exploit data, where "Companies make money and support their income flows through time" (Alcaíno, Arenas, & Gutiérrez, 2015, p. 12). There are six dimensions through which CDDBM may be classified: (i) key resources (data sources); (ii) key activities, (iii) value proposition, (iv) target customer segment, (v) revenue stream, and (vi) cost structure (Hartmann et al., 2014; Alcaíno et al., 2015). Based on these six dimensions, Annex 2 of this document explains the different classes of data-driven business models.

4 Defined herein as the human right protecting people against attacks that affect both their right to a private life and the freedom exercised in it. On this matter, see Constitutional Court, Judgment T-222, 1992.

5 Understood as the human right "that enables the owner of personal data to demand the personal data managers the access, inclusion, exclusion, correction, addition, update and certification of the data, as well as the limitation to its disclosure, publication or assignment possibilities pursu-

matter, the Article 29 Working Party of the European Union[6] has stated that, in the framework of personal data protection, big data is a cause for concern in the following four areas: (i) "the sheer scale of data collection, tracking and profiling, also taking into account the variety and detail of the data collected and the fact that data are often combined from many different sources"; (ii) "the security of data, with levels of protection shown to be lagging behind the expansion in volume"; (iii) "transparency: unless they are provided with sufficient information, individuals will be subject to decisions that they do not understand and have no control over"; and, (iv) "inaccuracy, discrimination, exclusion and economic imbalance" (EC, 2013, p. 45).[7] To summarize the concerns of the Working Party, the availability of large volumes of digital data, and our current capability to find correlations, can cause other personal data to be derived or inferred in order to profile a data subject (person). Our profile may be accurate or inaccurate, but it still affects us.[8] Decisions made based on this profile may be unfair or discriminatory, and may be made without us having security, knowledge, or control over what happens because of this data.

One example of the risks posed by big data to the right to privacy may be taken from the famous case of the Target retail chain, whose data analytics allowed it to figure out, based on her purchases, that a teen girl was pregnant even before her parents knew (Hill, 2012). On the other hand, the risks to data security are obvious in the Facebook/Cambridge Analytica scandal in which Facebook allowed the use of an application to

---

ant to the principles that inform the personal information databases management process." See Constitutional Court, Judgment T-729, 2002.

6 The Working Party, set up under Article 29 of Directive 95/46/CE of the European Parliament and the European Council, is the European Union's independent advisory body on data protection and privacy. It is comprised of the European data protection supervisor, the European Commission, and one representative of the Data Protection Authority from each member country of the EU. From the effective date of the General Data Protection Regulation (May 25, 2018), the Article 29 Working Party became the Data Protection European Committee.

7 The Working Party also mentioned the increased possibility of government surveillance as a concern; however, considering that this document focuses on the data-driven practices of private companies, we preferred to exclude government surveillance from the list of risks so as not to divert the reader's attention.

8 According to Frederike Kaltheuner, a working surveillance leads us to an Orwellian world, while inaccurate surveillance takes us to a Kafkaesque world (Joanne McNeil, n.d.).

collect information from 87 million user profiles around the world, which was then used by Cambridge Analytica to influence voters in the 2016 American presidential campaign and Great Britain's European Union membership referendum (Brexit). In the latter case, the United Kingdom Information Commissioner's Office finally concluded that Facebook failed to either safeguard its users' information or be transparent about how that data was harvested by others (Hern & Pegg, 2018). Finally, one example of discrimination resulting from the use of big data was revealed by research conducted at the University of Washington in 2015. When searching "C.E.O." in Google Image search, only 11% of the results showed women, whereas 27% of the executive officers of the United States are women (Kay, Matuszek, & Munson, 2015, pp. 1–10). Similarly, research conducted by Carnegie Mellon University, also published in 2015, found that Google's online advertisement system shows listings for high-income jobs more frequently to men than to women (Datta, Tschantz, & Datta, 2015, pp. 92–112).

It was precisely in response to this type of risk that the European Parliament and the Council of the European Union issued the General Data Protection Regulation (GDPR; Regulation [EU] 2016/679), which came into force on May 25, 2018, aiming to update the laws on personal data protection. Its purposes include an attempt to balance privacy and personal data protection with economic development and innovation. For this reason, the European Data Protection Supervisor, Giovanni Buttarelli, described the GDPR as a "radical update of the rulebook for the digital age" (McGuire, 2018).

Likewise, despite the absence of a comprehensive federal data-protection bill in the United States,[9] the State of California recently enacted the California Consumer Privacy Act (CCPA), resolution AB-375, to come into force in January of 2020. Just like the GDPR that inspired it, the CCPA aims to give Californians greater control over how companies collect and use their personal information. Thus, while it does not solve all current right-to-privacy problems, the CCPA is "a very good next step

9 On this matter, although there is no single federal data protection act, from March 2018 (partly due to various data breach scandals, such as Cambridge Analytica), all the U.S. states, including the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, implemented laws requiring companies to notify users if their personal information is being abused (Serrato, Cwalina, Rudawski, Coughlin, & Fardelmann, 2018).

as we work to empower citizens and protect democracy itself from out-of-control data collection" (McDonald, 2018, p. 4). The impact of this new bill is strengthened by the weight of California within the United States, as its large population and economy give its bills considerable influence in the rest of the country. For reasons of coherence and efficiency, companies may opt to comply with the laws of California in all other states as well. The headquarters of several large Internet companies are located in California, which makes this step even more significant.

How is Latin America facing these challenges? Unlike the European Union, "it seems that there is no uniform and coherent 'regional' approach in Latin America" (OAS, 2015, p. 1). This, despite the fact that Latin American Internet users ballooned from 278.1 million to 375.1 million between 2013 and 2018, with 387.2 million users expected by 2019 (Statista, 2018a). Regarding GAFAM, as of August 2017 Google held over 90% of the market share for search engines in Mexico, Venezuela, Argentina, Brazil, Bolivia, Colombia, Chile, and Peru (Statista, 2018b). The number of Facebook users in Latin America grew from 194.1 million in 2014 to 271 million in 2018, and is expected to reach 282.2 million by 2019 (Statista, 2018c). Similarly, between 2014 and 2018, the number of digital buyers of goods and services grew from 103.9 million to 147.2 million, with 155.5 million expected by 2019 (Statista, 2018d).

National initiatives to face this phenomenon in Latin America have not grown quite so fast. Brazil already has a personal data protection law,[10] based on the European model, aimed at addressing the challenges of the digital age. On the other hand, in Colombia, there have been no successful initiatives aimed at adapting the personal data protection regime to the age of big data and the digital economy.[11] This document is meant to explore these issues, including the following points: (i) whether the risks noted by the Article 29 Working Party are also latent in Colombia; and,

---

10 See Law 13.709 dated August 14, 2018.

11 The latest initiative on the matter was Bill 105/2015, which amended the scope of application of the Personal Data Statutory Law to make it applicable to the data controllers or processors who, even if not based or domiciled in Colombian territory, carry out any operation or set of operations on the personal data of people who were living, located, or domiciled in Colombia. However, this bill was ultimately withdrawn by its author.

if they are, (ii) whether our current personal data protection regime[12] and the authorities responsible for it are prepared to face them.[13]

In this text, we analyze the operations of a sample of 30 CDDBMs that collect data in Colombia. As will be explained below, we use the so-called "degree of consolidation" as the main criteria to select these companies, classifying them as "large Internet companies," "intermediate companies," startups, and "established companies." Based on this selection, and on a thorough review of the privacy policies[14] (Annex 1) of the main products offered by each of these 30 companies,[15] we analyze their opera-

---

12 In this text, "data protection regime" means the implementation of article 15 of the Political Constitution and Laws 1266/2008 and 1581/2012, and its regulatory decrees 1377/2013 and 886/2014, later included in Decree 1074/2015.

13 The competent authorities on personal data protection matters are the Department for the Protection of Personal Data of the Superintendence of Industry and Commerce, as the data protection authority, and the judges of the Republic, charged with ensuring the judicial enforcement of rights.

14 Understood as "the documents that explain how an organization handles any customer, client or employee information gathered in its operations" (Search Data Center, n.d.). In Colombia, privacy policies are legally referred to as "data treatment policies." Pursuant to article 25 of Law 1581/2012, these policies "are binding to those responsible and in charge thereof, and their breach shall result in the applicable penalties. In no case may the treatment policies be lower than the duties contained in this Law." Additionally, article 13 of Decree 1377/2013 provides that this document shall comply with the duty of informing, in a clear and simple language, at least the following:

1. Name or corporate name, domicile, address, email, and telephone number of the data controller.
2. *Processing* to which the data will be subject, and its *purpose* when it has not been made clear via a privacy notice. (italics added)
3. Rights of the data subject.
4. Person or area responsible for addressing requests, queries, and claims, before which the data subject may exercise their rights to know, update, rectify, and delete the information and revoke the authorization.
5. The procedure to enable the data subjects to exercise their rights to know, update, rectify, and delete information and revoke the authorization.
6. Effective date of the data treatment policy and term of the database.

15 Privacy policies should be distinguished from the so-called "terms and conditions" or "terms of use" that set forth the general standards for using the application or website, including the following: information on copyright, permitted and forbidden uses, terms of payment, and responsibility of the application or website owner, among others. Thus, although the "terms and conditions" or "terms of use" may refer to the privacy policies, they are not the same. See Terms Feed (2018).

tions using the following four categories: (i) data source, (ii) processing, (iii) purpose of the processing, and (iv) relationship with GAFAM. Then, we identify several typical digital-age practices that have not yet been sufficiently considered in the personal data regime currently applicable in Colombia, and whose regulation leaves vast room for improvement in comparison with the European GDPR and California's CCPA. Likewise, we identify several flaws in the capacity of the Colombian data-protection authorities to hold CDDBMs accountable and, consequently, we propose some corrective measures.

We hope that the contents of this document are useful for the legislators and public policymakers who must ensure that the Colombian personal data protection regime can meet the challenges of the digital age. Judges and the Deputy Superintendence for the Protection of Personal Data, in their different duties, must enforce the rights to privacy and personal data protection of those whose data is currently collected en masse by CDDBMs in Colombia, or abroad but with local effects. Besides these policymakers and upholders of the law, without prejudice to its content being used by CDDBMs, we invite members of civil society, academia, and citizens in general who are interested in the protection of personal data in the digital age to follow along with us on this exploration.

Clarification of the scope

Before continuing our analysis, three clarifications are needed. The examples used in this document of Europe's GDPR and California's CCPA are not necessarily meant as models to follow in Colombia; they are only used as guides for any possible solutions to be adopted. The GDPR and CCPA provide evidence that both the concept and the regulation of personal data protection can improve and evolve. On the other hand, we are aware that national regulation alone is not enough. Unlike oil, which is buried and clearly localized, data is a diffuse asset, generated everywhere, crossing borders with ease. Using the case of the European Union as an example, the ideal solution seems to be regional regulation, which in Latin America could be promoted from entities such as the Andean Community (CAN, for its acronym in Spanish) or the Inter-American Commission on Human Rights. Unlike national laws, regional regulation would allow Latin American countries to regulate a target market and, therefore, have more bargaining power with CDDBMs. Considering that a regional initiative is far from being a reality, however, in this document we chose to start

with a national approach, one aimed to at least maintain rights protection regarding personal data collected in Colombia.

Finally, thanks to the feedback received during the focus group[16] held on November 20, 2018, on the publication of this document in Spanish, we are also aware that state regulation is not the only possible option to deal with the challenges that big data poses for human rights; especially in a context of high technical complexity, where the enforcement always falls short of the rapid advancement of technology. Thus, in addition to state intervention, there are self-regulation measures[17] that CDDBMs may adopt — and are adopting — to ensure the protection of user rights in a complementary manner. Even the dynamics of the regulatory state model could be accepted, whereby "*the administrative law tends to be a regulation of self-regulation*, and of compliance with the private regulations to which the State attributes binding effects" (Restrepo, 2009, p. 72; italics added). Therefore, we could think about adopting self-regulation codes approved by the data protection authority, as well as certifying firms to verify compliance by CDDBMs. Likewise, digital literacy initiatives for citizens, as well as training data scientists on the responsible processing of data, may be promoted to ensure the protection of the subjects' rights.

Despite this, and without underestimating the value of these complementary solutions, we believe that state intervention cannot be dismissed, considering the following: (i) the technical complexity of the matter to be regulated is not an obstacle for the legislator and the regulator to receive advice from experts on the matter, as they do in equally complex matters, such as the regulation of the radio-electric spectrum and the electromagnetic spectrum; (ii) the high economic, technological, and social power that large Internet companies have acquired generates market failures that call on the state to intervene to "ensure that the market works properly for the benefit of everyone, not for those who occupy a special position of

---

16 The list of focus group attendees is included in Annex 3.

17 Based on the definition presented by the Ibero-American Data Protection Network (IADPN), the Constitutional Court (Judgment C-748, 2011) has defined self-regulation as "the set of rules adopted by the entities to define their policies and commitments regarding the processing of personal data" (IADPN, 2006). In turn, the European Commission (1998) has referred to self-regulation as the "set of data protection rules applying to a plurality of data controllers from the same profession or industry sector, the content of which has been determined primarily by members of the industry or profession concerned."

power due to their economic or technological predominance";[18] and, (iii) the state, not the companies, is the principal responsible for ensuring the protection of the human rights of its citizens.

On this third point, the right to the protection of personal data is a human right, recognized in several international human rights law instruments. In the case of the Universal System for the Protection of Rights, the right to the protection of personal information is closely related to the right to privacy, as set forth in article 12 of the Universal Declaration of Human Rights. It is also repeated in article 17 of the International Covenant on Civil and Political Rights (ICCPR). Based on these precepts, in 1998 the Human Rights Committee adopted Concluding Observation No. 16 on the right to privacy in the digital age:

> In order to have the most effective protection of his private life, 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. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

Likewise, initiatives such as the Guidelines for the Regulation of Computerized Personal Data Files[19] and the United Nations Resolution on the Right to Privacy in the Digital Age[20] have emerged from within the

---

18 Constitutional Court, Judgment C-150, 2003.

19 The Guidelines for the Regulation of Computerized Personal Data Files were approved by means of the United Nations General Assembly Resolution A/Res/45/95, based on the guidelines of the Organisation for Economic Co-operation and Development (OECD). The principles include lawfulness and fairness, accuracy, purpose-specification, interested-person access, non-discrimination, and security, among others.

20 The United Nations Resolution on the Right to Privacy in the Digital Age A/C.3/71/L.39 contains exhortations for both states and companies. It specifically calls on all states to respect and protect the right to privacy, including in the context of digital communications; to take measures to put an end to violations of those rights and to create the conditions to prevent such violations; to review their procedures, practices, and legislation regarding the surveillance and interception of communications, and maintain national surveillance mechanisms; to provide individuals whose right to privacy has been violated with access to an effective remedy; to develop and implement adequate legislation that protects individuals against il-

United Nations. Regarding the Inter-American Human Rights System, the right to the protection of personal data is interpreted based on Article 11 of the Inter-American Convention on Human Rights (IACHR). Furthermore, the most recent documents on the matter include the General Assembly Resolution AG/RES.2842 (XLIV-O/14) on Access to Public Information and Protection of Personal Data, whereby the importance of protecting the personal data and respecting the right to privacy is reaffirmed. After the General Assembly decided to entrust the formulation of different alternatives to regulate personal data protection to the Inter-American Juridical Committee, it produced some relevant documents on the matter, including the following: Privacy and Data Protection CJI/doc. 465/14; *Privacidad y Protección de Datos* CJI/doc. 450/14; and Privacy and Personal Data Protection CJI/doc. Clearly, although the right to the privacy of personal data ought to be respected by everyone, the obligation to ensure compliance falls mainly on the state.

legal and arbitrary treatments, namely when making decisions based on the automatized treatment, retention, or use of personal data by individuals, businesses, and private organizations.

1. SAMPLE OF DATA-DRIVEN COMPANIES IN COLOMBIA

The criteria for selecting the sample of 30 CDDBMs whose operations will be analyzed in this document included the "grade of consolidation" of the company, which fell into the following four categories: (i) large Internet companies; (ii) intermediate companies; (iii) startups; and (iv) established companies.

Regarding the large Internet companies, the sample includes five companies — Google, Apple, Facebook, Amazon, and Microsoft — usually grouped under the acronym "GAFAM," known for their capacity for innovation and their extensive investment capital (Colombia Digital, 2013). On the other end of the spectrum, we find companies, usually called startups, known for their young age, scalability, and exponential growth (Dorantes, 2018). Between these two categories, we have "intermediate companies," no longer at an early enough stage to be considered startups but not yet reaching the level of consolidation of the large Internet companies. Finally, the "established companies" include those created before the digital age that have adapted their business models to big data or have created new data-driven business models.

Considering that we are analyzing companies that collect data in Colombia, the criteria for selecting the "intermediate companies" included the ranking of their information and applications by market company App Annie (2018) for the top downloaded applications from the App Store (see iPhone Top App Matrix; Annex 4) and Google Play (see Google Play Top App Matrix; Annex 5) in Colombia. We reviewed and tabulated the most downloaded applications from the App Store and Google Play

during the first five days of July, August, and September of 2018,[21] the results are shown in Table 1.

Table 1
Top 10 Most Downloaded Applications in Colombia (First five days of July, August, and September 2018)[22]

App	Times shown in the top 10 downloaded applications in Colombia	Company
WhatsApp	30	Facebook Inc.
Tinder	30	Match Group, LLC.
Messenger	24	Facebook Inc.
Facebook	23	Facebook Inc.
Instagram	17	Facebook Inc.
Facebook Lite	15	Facebook Inc.
Netflix	15	Netflix International B.V.
Deezer	15	Deezer SA
Google Drive	15	Google LLC.
YouTube	13	Google LLC.
LinkedIn	10	Microsoft Corporation
Messenger Lite	2	Facebook Inc.
AliExpress	2	Alibaba Group
Joom	1	SIA Joom (Latvia)
30 Day Fitness Challenge	1	Bending Spoons S.p.A.
8fit Workouts and Meal Planner	1	Urbanite Inc.

SOURCE: Based on information from App Annie (2018).

As shown in Table 1, nine of the top 16 apps downloaded in Colombia (56%) are owned by GAFAM companies (WhatsApp, Messenger, Facebook, Instagram, Facebook Lite, Google Drive, YouTube, LinkedIn, and Messenger Lite). However, seven other companies also own popular applications and have therefore been included in our "intermediate companies" group. Likewise, we included four other companies whose

21 Although we intended to cover a longer time span, the free version of App Annie only allowed us five days per month.

22 These results do not include games applications, nor DirectTV and Selección Colombia, which were massively downloaded during the 2018 FIFA World Cup.

applications (Spotify, Waze, Uber, and EasyTaxi), even if not part of the top 10 most downloaded applications during those three months, are very popular in the country.

The selection criteria for startups included their affiliation to either Team Startup Colombia (2017) or INNpulsa Colombia, the dynamic Colombian government agency engaged in promoting corporate growth through innovation. The first is a group of digital ventures that, according to the Ministry of Information and Communications Technologies, "are at the level of the main global startups thanks to their good practices, achievements, traction, sales, growth, and immersion into new markets, and are a reference for Colombians at a national and international level" (Team Startup Colombia, 2017). The second is a venture portfolio, which, according to INNpulsa Colombia (n.d.), includes the best startups to invest in the country. This sample does not include all the companies that are part of these two portfolios, but rather those with a clearly delineated privacy policy. Although not included in any of these portfolios, we have likewise included two more companies that offer applications (Biko, Duety) whose data processing model is worth studying.

Finally, in choosing "established companies," we selected the largest companies in Colombia in each of the following sectors: mass market, retail (Portafolio, 2017), insurance (BNamericas, 2017), financial (El Tiempo, 2017), and telecommunications (La Nonsoque, 2018). Table 2 shows our sample of 30 CDDBMs, including their products and a brief company description.

Clearly, this sample of CDDBMs does not intend to be representative, but is illustrative of the types of companies currently collecting personal data in Colombia. It omits many companies whose personal data processing is worth analyzing. However, examining the operations of these 30 companies offers sufficient information to illuminate the degree of preparedness of our legal data protection regime and of those charged with upholding it, considering the current and coming challenges of the digital age.

Table 2
CDDBMs Being Studied

Category	CDDBM	Products[23]	Description
Large Internet companies (5)	Google LLC.	Google Search Google Drive Google Maps YouTube	Company specializes in products and services related to the Internet, software, electronic devices, and other technologies
	Amazon Inc.	Amazon.com	E-commerce and cloud computing services company
	Facebook Inc.	Facebook Facebook Lite Messenger Messenger Lite Instagram WhatsApp (with its own privacy policy)	Company offering social networking and social media services online
	Apple Inc.	iPhone iPad Apple Watch iCloud	Company engaged in the design and production of electronic equipment, software, and online services
	Microsoft Corporation	Windows Office 365 Microsoft Azure Microsoft Dynamics 365 Microsoft Intune Windows Server SQL Server Visual Studio System Center StorSimple Bot Framework Cortana Skills Kit Botlet Store Bing Cortana Microsoft Translator SwiftKey Xbox MSN Mixer Microsoft Store Silverlight Outlook LinkedIn (with its own privacy policy)	Company engaged in offering services, websites, applications, software, servers, and devices

23 Although we intended to cover a longer time span, the free version of App Annie only allowed us five days per month.

Category	CDDBM	Products	Description
Intermediate companies (11)	Match Group, LLC.	Tinder	Company that provides a geo-social application that allows users to communicate with other people based on their preferences to chat and set up dates or encounters
	Netflix International B.V.	Netflix	Entertainment company that provides streaming of on-demand multimedia content on the Internet for a fixed monthly fee
	Deezer SA	Deezer	Website and application that offers unlimited music on a subscription basis
	Alibaba Group	AliExpress	Online store offering products from small companies from China and other countries to international buyers
	SIA Joom (Latvia)	Joom	Online store that offers Chinese products at very low prices
	Bending Spoons S.p.A.	30 Day Fitness Challenge	Fitness application for home workouts
	Urbanite Inc.	8fit Workouts and Meal Planner	Fitness application that works as a personal trainer, preparing the personal training and nutrition plan of the user based on self-defined training goals
	Spotify AB	Spotify	Company that provides a multi-platform application used to play music via streaming
	Waze Mobile Limited	Waze	Company that provides a GPS navigation application
	Uber B.V.	Uber	Company that provides a private transport network through software that connects riders and drivers
	EasyTaxi Colombia S.A.S.	EasyTaxi	Application that allows users to request a taxi service and track it in real time

Category	CDDBM	Products	Description
Startups (9)	1DOC3 S.A.S.	1DOC3	Web platform where doctors answer health queries anonymously and for free
	Acsendo S.A.S	Acsendo	Cloud computing software that helps to evaluate the work environment and the performance of organizations
	Fluvip S.A.S	Fluvip	Virtual platform that connects large brands with influencers around the world, allowing them to identify the appropriate influencers for each campaign and brand
	Rappi S.A.S	Rappi	Application that offers a broad range of products and services available for delivery by using "rappitenderos"
	Cívico Digital S.A.S	Cívico	Virtual platform on which citizens construct their ideal city by sharing information through quests, earning points that they can exchange for benefits
	Inversiones CMR S.A.A.	Domicilios.com	Online orders through the Internet or mobile applications
	IoT Services Inc.	Ubidots	Platform based on the cloud, which integrates information from different sources and helps in the process of organizing the information collected
	Biko Development Inc.	Biko	Mobile application that promotes bicycle use in cities by rewarding users with points that can be exchanged for goods and services
	Duety S.A.S	Duety	Social network for couples to earn "matripuntos"

Category	CDDBM	Products	Description
Established companies (5)	Unilever PLC Unilever N.V.	Unilever Group	Mass-market multinational company that produces and sells products under 400 brand names around the globe
	Almacenes Éxito S.A.	Grupo Éxito	Retail multinational
	Seguros Generales Suramericana S.A.	SURA	Insurance company
	Grupo Aval Acciones y Valores S.A.	Grupo Aval	Colombian corporate conglomerate engaged in a broad range of activities, mainly in the financial sector
	Telmex Colombia S.A.	Claro	Telecommunications services company

SOURCE: Authors.

2. HOW COMPANIES COLLECT DATA IN COLOMBIA

Based on a review of the privacy policies of the products offered by the 30 CDDBMs included in the sample (Annex 1), we analyzed their method of operation based on the following four categories: (i) data source, (ii) processing, (iii) purpose of the processing, and (iv) relationship with GAFAM. As shown below, the description of these categories combines terminology from both personal data protection and that usually used to describe the data-driven business models (Hartmann, Zaki, Feldmann, & Hartmann, 2014; Alcaíno, Arenas, & Gutiérrez, 2015; see Annex 2).

Data sources

Most CDDBMs included in the sample have three sources of data: (i) the data provided by the user/client; (ii) the data collected through web tracking; and (iii) the data provided by "strategic partners."

Data provided by the user/client is usually information entered when creating an account or profile (e.g., name, password, telephone number), using the service (e.g., destination, location), making a purchase (e.g., items acquired, payment information, bank accounts), or uploading content to the platform or application. However, in the case of WhatsApp, its privacy policy states that, except under exceptional circumstances,[24] the content of messages sent by the user through the application is not

24 i.e., "(i) If a message cannot be delivered immediately, we may keep it on our servers for up to 30 days as we try to deliver it. If a message is still undelivered after 30 days, we delete it; (ii) when many people are sharing a popular photo or video, we may retain that content on our servers for a longer period of time."

stored on Facebook Inc. servers, but on the user's own device. Similarly, the privacy policy of the 30 Days Fitness Challenge app states that "the application provider does not store any information regarding what you write while using the application."

In some cases — such as Facebook, Tinder, 1DOC3, Unilever, or Sura — the information provided by the user/client includes sensitive data (also called "specially protected data" or "special categories of personal data"), such as those related to religious beliefs, political opinions, ethnic or racial origin, philosophical beliefs, unionization, interests, health, or facial recognition. In other cases, such as AliExpress, the provision of this information is optional, and its policy provides that "if you prefer not to provide such information, the use of our services and products will not be affected." In turn, in the case of Unilever, its privacy policy states, "in some cases, you may have requested services or products that do not directly imply the collection of special categories of data, but which may imply or suggest your religion, health or other special categories of data." In contrast, companies such as Acsendo expressly clarify that "we do not collect, store, organize, use, transmit, transfer, update, rectify, delete, eliminate or manage sensitive information." Similarly, EasyTaxi's privacy policy reads, "None of the information we process is considered to be sensitive."

Data collected through web tracking usually includes data on the applications, browsers, and devices used by the user/client (log data; e.g., IP address, version and type of device and browser, time zone settings, language preferences, type and versions of browser plugins, Internet service provider [ISP], connection speed), and on its activity on the respective platform or application (online data; e.g., times and dates of access to the services, products visited or searched, purchase information, hashtags used, persons or groups with whom you interact, mouse clicks, scrolling through the page or number of times you mouse over certain elements, the origin URL, forms of leaving the website, and the URL you visit next). Likewise, it includes data on the location of the user/client (even when the application is not being used), which may be determined through the GPS, the IP address, sensor data of the device used, Wi-Fi hotspots, cell towers or Bluetooth-enabled devices near it, or other devices that are nearby or share the same network. However, in the case of Apple, its privacy policy is that "unless you provide consent, this location data is collected anonymously in a form that does not personally identify you." This anonymity should be a standard, in our opinion.

Alarmingly, unlike the data provided by the user/client, some companies — such as Duety and Apple — consider that data collected through *web tracking is non-personal information*, which is not related to the user/client, but rather with the IP address and similar identifiers of the device used. For example, Duety states, "We do not process Log Data as personal information, and we do not use it in association with other personal information; however, we might add, analyze and evaluate it for the same purposes as aforementioned for unidentifiable personal information." Apple, however, will process the IP address and similar identifiers as personal information "when these are treated as such by the local laws." Civico states the following policy on the protection of personal data:

> Although we process this information as personal data, you must be aware that *CIVICO only uses these data globally*, that is, to inform our partners and associates on how users are, *considered collectively*, use our services so our partners may also understand how frequently people use their services and our services. (Italics added)

Similarly, the privacy policy of the application 8fit Workouts and Meal Planner says that

> ... we are unable and do not attempt to draw any conclusions about your identity from the data collected. Your device's IP address and the other information listed above are used by us for the following purposes: to ensure that a trouble-free connection can be established; to ensure the convenient use of our services; to evaluate system security and stability; other administrative purposes.

In contrast, LinkedIn clearly acknowledges, "we use log-ins, cookies, device information and Internet protocol (IP) addresses to identify you and log your use."

Regarding *data provided by strategic partners*, the policies are less homogeneous; the most common include provisions such as these: (i) third parties who provide any service on behalf of the company (e.g., carriers); (ii) marketing or advertisement companies who provide advertisement and research services (in which case details on the success of a campaign on own or third-party websites is transferred); (iii) third-party platforms on which the company has accounts, such as when users click the "Like" button on Facebook, or the +1 button on Google+; (iv) the "third-party

data enrichment providers," who process and draw conclusions on the personal data held by the CDDBM; (v) companies to whom they provide services such as, in the case of Google, the websites using advertisement services such as AdSense, include analysis tools such as Google Analytics, or embed YouTube video content; or, in the case of Uber, those using the Uber API; and (vi) credit bureaus, who use applications and platforms to offer credit and financial services to certain users/clients.

Regarding this data exchange, several companies, such as Facebook and Fluvip, demand that all third parties have legitimate rights to collect, use and share this information. Spotify, on the other hand, mentions that "we will use this personal data either where you have provided your consent to the third party or to Spotify to that data sharing taking place *or where Spotify has a legitimate interest* to use the personal data in order to provide you with the Spotify Service" (italics added). In turn, in its privacy policy, updated on April 24, 2018, WhatsApp mentions that "We protect the data obtained from third parties pursuant to the practices described on this statement, in addition to the additional restrictions set by the data source."

In addition to these three data sources, we identified the *acquisition of information from external data providers* (Acxiom, Oracle, etc.) as a fourth source, although less used (or, at least, less included in the privacy policies). Also called "online and offline data brokers," these are third parties who sell data on the actions and purchases made by users/clients inside and outside of the Internet. However, it is not clear if these data brokers only provide aggregated statistical and demographic information attributed to the users based on their allocation in certain statistical groups or their use of services, or if they also provide personal data that enable individualizing the holder. For example, in its privacy policy, Biko recognizes the "purchase [of] third-party marketing data," without specifying if these are granular or aggregate data. More clearly, Microsoft mentions that one of its sources is "data brokers from which we purchase demographic data to complement the data we collect." Likewise, it is not clear how this third-party data is transferred. In the case of Facebook, for example, its privacy policy, updated on April 19, 2018, provided that:

> Facebook collaborates with a select group of third-party data providers to help business connect with people who might be interested in their products or services. […] Today, many businesses work with third parties, such as Acxiom, Oracle, Data

> Cloud (formerly DLX), Epsilon, Experian and Quantum, with the purpose of managing and analyzing their marketing initiatives. [...] The third party *provides* Facebook with information, so the platform may connect the clients with the offers. (Italics added)

Additionally, Facebook data providers agree to facilitate an opt-out form on their websites so that users can choose not to receive personalized advertising based on this data. However, the available links to the forms at the time we wrote this book did not include one for Colombia.

Finally, some of the companies included in the sample also use *freely accessible web data,* although to a lesser extent (Google for web crawling, Apple for public access sources, Fluvip for social media, and Netflix and Microsoft for open government databases), *sensors and devices* (Ubidots, Biko), and crowdsourcing[25] (Facebook, Cívico, Waze).

Processing

The processing of personal data by CDDBMs included in the sample seems to be uniform, mainly focusing on collection and analysis. *Collection* is usually done through the following technology tools:

1. *Own or third-party cookies* are small files containing a chain of characters sent to the user's computer whenever they enter a website. When the user visits the site again, the *cookie* allows the site to recognize their browser. Cookies may store user preferences and other types of information.
2. *Advertisement identifiers* are similar to cookies, but found in various mobile devices and tablets (for example, the "identifier for advertisers" or IDFA for Apple iOS devices, and "Google advertisement ID" for Android devices), and in some multimedia players.
3. *Pixel tags* (web beacons, clear .gif or web bugs) are a type of technology found in a website or in the body of an email that allows monitoring certain activities, such as website visits or when an email is opened.
4. *Software development kits* (SDKs) are small fragments of code included in the apps and work like cookies and pixel tags.
5. *Browser web storage* is a local storage technology that allows websites to store data on the browser of a device.

---

25 For the Waze application, one of its data sources (combined with web tracking) is user contributions on the status of roads and traffic jams.

6. *Application data cache* is a data repository in a device that allows the execution of a web application without an Internet connection, and faster loading times of the content to improve the performance of the application.
7. *Server registries* are servers of the CDDBM that automatically register requests made by website users when they visit.
8. *Tracking URL addresses* is done via personalized links that help the company understand where the traffic on its websites comes from.

Companies such as Apple, 1DOC3, Biko, Tinder, Netflix, and Microsoft specify — based on the United Kingdom International Chamber of Commerce Cookie Guide (except for Microsoft, which names them differently) — the types of *cookies* used to collect information. Within the universe of these files, the most common are these:

1. *Strictly necessary cookies* are essential in order to enable the user to move around the website and use its features.
2. *Performance cookies* allow for quantifying the number of users, how they use the websites, and measuring and conducting the statistical analysis of how users use the service offers. This data may be used to help optimize the websites and make them easier to navigate. These cookies are also used to enable the affiliates of a company to know if users reached one of their websites from an affiliate, and if their visit resulted in the use or purchase of any of its products or services, including information about the product or service acquired.
3. *Functionality cookies* allow websites to remember the decisions made by a user while browsing, and recognize them upon the user's return. For example, they may store the geographical location of a cookie to show the region-specific website to a user. It may also remember the preferences, such as font size, font type, and other configurable elements of the site. They may also be used to monitor the highlighted products or videos seen, and prevent their repetition.
4. *Targeting or advertising cookies* allow for analyzing the Internet browsing habits, and thus, manage the offer of the advertisement spaces on the websites based on the user's navigation profile, adapting the content of the advertisement to the content of the service requested or used by the website user.
5. *Interaction or social networking cookies* (also called social plugins, such as Facebook's "Like") allow the user to show their interest on a

page or recommend it, and may collect information even if the user does not use them.

Apple clarifies that *performance* and *functionality cookies* "don't collect information that identifies you." While we believe that in principle this is good, we must consider the latent possibility that the holder of this data may be easily identified based on a combination of various apparently impersonal data.

In turn, companies such as AliExpress, Duety, Tinder, or the owner of the 8fit Workouts and Meal Planner app also use the following classifications: (i) *permanent/persistent cookies* used to save the login information to sign-in in the future; (ii) *session cookies* used to enable certain characteristics of the site and the application to better understand how the user interacts with them, and to monitor aggregate use and the web traffic that led the user to the site and the application. Unlike persistent cookies, session cookies are deleted from the user's computer upon logging out from the website or application. Furthermore, Deezer recognizes the use of *third-party cookies* by mentioning, "we authorize some of our commercial partners to place advertising data collection systems on the services or advertisements shown. The insertion and use of collection systems are subject to the privacy policies of said third parties."

Analysis is usually *descriptive* and aimed at segmenting users and audiences according to their tastes, interests, and connections, or *prescriptive* and aimed at improving the user's experience on future visits. Regarding the technology tools to conduct these analyses, the level of detail included in the privacy policies is very low, and sometimes nonexistent. Among those that provide some information, Rappi refers to "business intelligence or data mining tools," Microsoft refers to "automated processes," and AliExpress refers to "use of automated data with machine learning purposes." In turn, Google mentions Google Analytics and automated analysis systems and algorithms, while Netflix refers to "recommendation algorithms." With a greater degree of specificity, 1DOC3 and Ubidots refer to the IBM Watson Natural Language Classifier service on IBM Bluemix, which classifies user queries in real time, producing specific content for repeated questions and sending new requests to real people. Finally, Unilever uses "game simulations of science-based behavioural assessments and data science techniques." Lastly, it is interesting to note that Apple, clearly influenced by the GDPR, mentions in its privacy policy that

it "does not take any decisions involving the *use of algorithms* or *profiling* that significantly affects you" (italics added).

Finally, the only company to recognize the *sale or trade of personal data* openly is Cívico. In contrast, Amazon, Facebook, Joom, Uber, and Waze all expressly mention that they are not engaged in selling the personal information of their clients to third parties. However, this is not an obstacle for these companies (except for Joom), to mention that in the event that the company is acquired by a third party, the personal data of its users/clients will be one of the assets transferred. Google, Amazon, Ubidots, Spotify, Waze, and LinkedIn positively ensure, however, that the information delivered to the purchaser will continue to be subject to the commitments acquired under any pre-existing privacy notice until the user is notified. Furthermore, in a more protective way, AliExpress and Netflix provide that "in connection with any reorganization, restructuring, merger or sale, or other transfer of assets, we will transfer information, including personal information, provided that the receiving party agrees to respect your personal information in a manner that is consistent with our Privacy Statement."

Purposes

The most common purposes for which CDDBMs process personal data are as follows: (i) provide goods or services; (ii) communicate and interact with the user; (iii) develop new goods or services based on the identification of needs; (iv) manage sweepstakes, contests, discounts, or other offers; (v) conduct market research; (vi) *offer personalized content (including advertisements)*; (vii) measure the performance of the content; (viii) prepare studies and research; (ix) *share information with third parties*. In the latter case, the possible third parties with whom information is shared include the following: (i) advertisers; (ii) *companies in the same group or subsidiaries, affiliates or associates;* (iii) *third-party applications that connect to the company's application or are used to sign-in;* (iv) service providers on its behalf; (v) *academic researchers*; (vi) measurement partners; (vii) *public authorities*; and, eventually, (viii) possible purchasers of the company.

Offering a high level of transparency, we note that the privacy policy for the 8fit Workouts and Meal Planner app includes the names of the third-party applications connected to it, or used to sign-in, as well as the measurement partners with whom information is shared. This is very much in contrast to the rest of CDDBMs studied, which mention

"third-party applications" and "measurement partners" generically. The case of WhatsApp is interesting because, when sharing user information with third-party services and Facebook companies (the corporate group to which it belongs), it specifies that "when we share information with third-party service providers and the Facebook companies in this capacity, we require them to use your information on our behalf in accordance with our instructions and terms." Likewise, AliExpress specifies, "these service providers must abide by our data privacy and security requirements and are only permitted to use your Personal Data in connection to the purposes specified above, and not for their own purposes." In turn, LinkedIn provides that:

> We do not share your personal data with any third-party advertisers or ad networks for their advertising except for: (i) hashed or device identifiers (to the extent they are personal data in some countries); (ii) with your separate permission (e.g., lead generation form) or (iii) data already visible to any users of the services (e.g., profile). However, if you view or click on an ad on or off our site or apps, the ad provider will get a signal that someone visited the page that displayed the ad, and they may through the use of mechanisms such as cookies determine it is you. Advertising partners can associate personal data collected by the advertiser directly from you with our cookies and similar technologies. In such instances, we seek to contractually require such advertising partners to obtain your explicit, opt-in consent before doing so.

In addition to the processing purposes mentioned above, Cívico, also includes the

> …creation of a *data base that may be subject to trade*, consultation, transmission or transfer of personal data to risk assessment centers and other databases of different nature, owned by, or managed by, Cívico or by third parties with whom Cívico has commercial, contractual or operational relationships with the purpose of allowing Cívico or our partners, third parties and commercial associates to offer and promote products and services. These third parties' recipients of the databases and the personal data may be located in Colombia or abroad. (Italics added)

Likewise, the purposes of the processing carried out by Duety include the "assignment of databases." Unilever's processing purposes include *making automated decisions,* understood as those exclusively made through automated means, where no humans are involved in the decision-making process related to personal data. According to their privacy policy, clearly influenced by the requirements of the GDPR,

> *…we will not make decisions based solely on automated decision making that have significant impact on you.* If we do so we notify you and provide you with clear information about our decision to rely on automated processing to make our decision and our lawful basis for doing so. You have the right not to be subject to a decision which is based solely on automated processing and which produces legal or other significant effects on you. In particular, you have the right: (i) to obtain human intervention; (ii) to express your point of view; (iii) to obtain an explanation of the decision reached after an assessment; (iv) to challenge such a decision. (Italics added)

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

The relationship of the CDDBMs with GAFAM is, essentially, of four types: (i) the app or website allows signing in via a third party or social network (including, but not limited to, Facebook); (ii) the use of social buttons on its page or application provided by Twitter, Google+, LinkedIn, or Facebook; (iii) the use of Google Analytics, a Google service that uses cookies and other data collection technologies to gather information on website and service use to analyze trends; and/or (iv) Google companies are among their advertising partners. While the first relationship allows GAFAM to provide personal data to CDDBMs, the others enable GAFAM to access the information held by the former. For example, in the case of AliExpress, it provides that "if you are registering an AliExpress account through social media platforms such as Facebook or Twitter, we may collect your account name and profile photo at those platforms."

The particular case of 1DOC3 is interesting, as it joined Facebook's *Internet.org initiative* to provide accessible Internet services to less developed countries. Additionally, none of the "established companies" seem to have any relationship with GAFAM, at least not beyond having profiles on their different sites.

Finally, there are products (such as WhatsApp, YouTube, or LinkedIn) that, although they apparently do not belong to GAFAM, are part of their corporate groups and, to that extent, permanently share information with them. For example, WhatsApp's privacy policy provides that: "WhatsApp receives information from, and shares information with, the Facebook family of companies. We may use the information we receive from them, and they may use the information we share with them, to help operate, provide, improve, understand, customize, support, and market our Services and their offerings."

As we have seen, several data sources, processing methods, purposes, and relationships developed by the CDDBMs studied raise concerns similar to those addressed by the Article 29 Working Party, quoted above. The emergence of cookies as the main data collection tool raises questions about the *massive scale of data collection and monitoring* that these companies have reached considering the variety and detail of data they may collect. As well, the large number of data sources accessed by these companies raises questions about the *countless possibilities of data combinations* available to them. Likewise, the information exchange relationships between the different corporate groups, as well as between GAFAM and other CDDBMs, raise still more questions about the *security of the data collected*. While privacy policies provide the user/client with assurance about the security systems used by the respective product, they do not do so regarding the products or companies with which the information will be shared, and which do not seem to have any commitment whatsoever to the owner of the data. The scant information available on the data analysis methods used by the CDDBMs, particularly algorithms used, raises concerns about the *transparency standards* demanded from these companies. Finally, the increasing use of profiling to provide personalized content and, in some cases, to enable automated decision-making, creates obvious risks *for the development of equality and non-discrimination of the data owners.*

Thus, encouraged by these common concerns, and with the same aspiration as the European Union to balance innovation and economic development with data protection and the values of a democratic society, next we will evaluate how our legal regime and its authorities are prepared to address these new dynamics of the digital age, hold CDDBMs accountable, and prevent privacy risks.

3. FACING THE DIGITAL AGE WITH THE PERSONAL DATA PROTECTION REGIME

In light of how the companies we studied operate, we will now examine the level of preparedness of the Colombian legal regime and its authorities to face these risks and hold these companies accountable regarding their use of personal data collected in Colombia.

Scope of the data protection regime

In Colombia, the personal data protection regime is established both in article 15 of the Political Constitution (PC), and in two statutory laws. Article 15 of the PC provides that:

> All individuals [...] have the right to know, update, and rectify information collected about them in data banks and in the records of public and private entities.
>
> Freedom and the other guarantees approved in the Constitution will be respected in the collection, processing, and circulation of data.

To further this constitutional provision, and based on the vast jurisprudence on the matter, Statutory Law 1266/2008, which regulates the protection of personal data regarding financial, credit, commercial, and services information, as well as that coming from other countries, was enacted. Unlike the preceding sectoral law, Law 1581/2012, enacted some time later, generally regulates the processing of personal data in Colombia and includes provisions regarding the purpose, liberty, accuracy or quality, transparency, restricted access and circulation, security, and confidentiality with which personal data is treated. Additionally, it provides for the

rights of the personal data subjects, the procedures to enforce said rights, and the duties of those responsible for their processing. This law also regulates the legality conditions of personal data processing, especially the processing of sensitive data and that of children and teenagers as special categories. Finally, Law 1581/2012 also provides mechanisms for monitoring and enforcing compliance with the law.

Based on a detailed study of the contents of Law 1581/2012 and of the aforementioned behaviors, however, there are several issues, mainly related to the digital age, not covered by the laws currently applicable in Colombia: (i) inferred sensitive data, (ii) data linked to the IP, (iii) use of cookies, (iv) web crawling, (v) data commercialization, (vi) personalized contents, and (vii) automated decisions. Likewise, although Colombia's current regime considers the use of data for academic research purposes, it is clear that the regulations governing research were not established for the digital age. The current laws require the prior, free, informed consent of the data subject to consider consent valid, which are toothless nowadays. The problem of non-existent or deficient regulation of digital age matters lies in the consequent lack of protection for the subjects of the personal data processed. Considering the legal principle that anything not expressly forbidden is allowed, in principle, the data sources, their processing methods, and their purpose are allowed with no limitations in the digital age. Many digital matters are not regulated in the Colombian regime; others, although regulated, require revision to ensure that the rights to privacy, the protection of personal data, equality and non-discrimination, and their related freedoms (of expression, of association, to personal identity, among others) of the data subjects.

What is not, but should be, regulated

- *Inferred sensitive data and data leading to inference*

In Colombia, the concept of "sensitive data" is defined under article 5 of Law 1581/2012. According to this article,

> Sensitive Data is that which affects the privacy of the Owner or whose undue use may cause discrimination, such as *those disclosing* racial or ethnic origin, political orientation, religious or philosophical convictions, membership in unions, social or human rights organizations, or that promotes the interests of any political party or that ensures the rights and obligations of opposition political parties, as well as information related to health, sex life and biometric information. (Italics added)

This concept does not establish, per se, that sensitive data includes only that delivered by the subject or source.[26] Therefore, sensitive data could also include information inferred from other data, which may *disclose* the religion, health, or other special categories of the subject. In this light, the processing of inferred data, and other sensitive data, would be prohibited. Exceptions to this prohibition, contained in article 6, are as follows: (i) that the subject had expressly authorized said processing, except when said authorization is not required by law; (ii) that the processing is necessary to protect the vital interests of the subject, and they are physically or legally incapacitated, in which case the legal representatives must provide their authorization; (iii) that the processing takes place in the course of legal and duly guaranteed activities by a charity, NGO, association, or any non-profit organization whose purpose is political, philosophical, religious, or union-related, provided they exclusively refer to members and not to persons with whom they communicate regularly pursuant to their purpose, and provided the data is not provided to third parties without the authorization of the subject; (iv) that the processing refers to the data required for the recognition, exercise, or enforcement of a right during a legal proceeding; or (v) that the processing has a historical, statistical, or scientific purpose, provided that the data is anonymized.

But what happens when non-sensitive data (e.g., purchases made on Amazon.com) *that, together with other data*, allow sensitive data to be inferred (e.g., the ethnicity or sexual orientation of an individual)? In our opinion, they should also be considered as sensitive since, ultimately, they also "disclose information that affects the privacy of the subject, or whose undue use may result in discrimination." California's CCPA, which, although it does not expressly refer to sensitive inferred data, does at least include inferred data in the definition of personal data. Section 1798.140(o) states that personal information includes the following:

> (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological

---

26 *Personal Data Study*: *The Emergence of a New Asset Class*, published by the World Economic Forum (WEF, 2011), clearly establishes that the concept of personal data not only includes the data "voluntarily" provided by the owner, but also: (i) the *observed data*, collected by recording the actions of owners; and (ii) *inferred data*, obtained from analyzing the volunteered and observed data.

> trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

The practical consequence of this provision is that, by considering them as personal data, the inferences made about a person are subject to the guarantees of the right to data protection, including the need to request authorization from the data subject to process them in any way and to notify the subject of the purpose of said processing.

In Colombia, however, the current definition of both personal data and sensitive data included under the law is not expressly considered in this situation. Of course, the current law was formulated at a time when it was not expected that personal data would permit inferring new information about the subject, at least not with the accuracy of today's data analytics. Presently these data can be treated with greater freedom than sensitive data, despite the risks their processing may create for the privacy and right to equality of their subjects.

• *Data from Internet protocols (IP) and similar identifiers*

In Colombia, article 3(c) of Law 1681/2012 defines personal data as "any information *related to or that may be traced to* one or several *determined or determinable individuals"* (italics added). Thus, the question arises, are IP addresses and similar identifiers linked, or can they be linked, to one or several determined or determinable individuals? Section 30 of the European Union's GDPR provides that:

> *Natural persons may be associated with online identifiers* provided by their devices, applications, tools and protocols, such as *internet protocol addresses*, cookie identifiers or other identifiers such as radio frequency identification tags. *This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.* (Italics added)

In turn, article 4(1) of the GDPR defines personal data as

> …any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an *identifier* such as a name, an identification number, location data, an *online identifier* or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Italics added)

Thus, European regulations consider that online identifiers — including IP addresses — allow the direct or indirect determination of a person's physical identity (by *combining* it with unique identifiers and other data received by the servers). Furthermore, before the enactment of the GDPR, and pursuant to Directive 95/46/CE, the Article 29 Working Party considered IP addresses as data related to an identifiable person. In this regard, in the working document "Privacy on the Internet: An Integrated EU Approach to Online Data Protection," issued November 21, 2000, the Working Party declared that

> Internet Access Providers and Managers of Local Area Networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases *there is no doubt about the fact that one can talk about personal data in the sense of Article 2 a) of the Directive.* (EC, 2000; italics added)

Thus, considering that in other parts of the world it is understood that IP addresses allow direct or indirect identification of an individual, based on article 3(c) of Law 1581/2012, we could argue that these are related to a determinable individual and, to that extent, would be included in the definition of personal data. Consequently, the provisions of Law 1581/2013 would apply to the processing of said identifiers.

Bodies of law such as California's, however, pose even more certainty on this matter. In the CCPA, the definition of "personal information" includes — in addition to biometrics, psychometrics, geolocation data, and Internet browsing history — identifiers such as real name, alias, mailing address, unique personal identifier, online identifiers (IP address), email address, user name, social security number, driver's license number, passport number, or similar identifiers.[27] Such legal provisions allow much more certainty in arguing that IP addresses are, in fact, personal data.

So, what happens with the data related to these identifiers? Should it also be considered as personal data? For example, consider Google searches or browsing items on the Almacenes Éxito website, which save a "digital track" through cookies associated to an IP, even if the user has not

27 See letter Section 1798.140(o) of the CCPA.

signed in. In our opinion, this information, although not directly linked, *could be linked to determinable persons* since online identifiers may be associated with determinable persons; therefore, they should be included in the definition of personal data covered under Colombian law. Until Colombia expressly provides, or a judge interprets, or even a regulatory authority[28] issues a guide on the matter clarifying that IP addresses and their related information are personal data, however, each CDDBM is free to determine whether to treat them as personal data or not. Clauses such as Apple's, which states that IP addresses and similar identifiers will be treated as personal information "to the extent that [these] are considered personal information by local law," would be relatively useful. The absence of express regulation results in cases such as that of LinkedIn, which allows sharing their users' IP addresses with advertisers because, although they do not share personal user data with any advertiser or ad network, they do make an exception for "(i) hashed or device identifiers (to the extent they are personal data in some countries)."

• *Cookies*

According to our own data protection authority, "there is no specific regulation on the use of cookies in Colombia" (SIC, 2016b). Generally, article 3(g) of Law 1581/2012 includes data collection as one of the operations that constitute the processing of personal data. Thus, the obligations and guarantees set forth in the law would theoretically apply to data collection by cookies; however, the law does not refer to the tools used for collecting data. To that extent, it is understood that any type of tool that does not violate the constitution or the law may be used to collect data, including cookies. Additionally, this implies that any kind of cookie may be implemented regardless of whether they are session, permanent, own, third

28 Regarding the positions that the Office for the Protection of Personal Data of the Superintendence of Industry and Commerce may take in its capacity as data protection authority, note, "the opinions issued by entities in response to a right to petition with consultation purposes do not constitute authorized interpretations of the law or of an administrative act. They cannot replace an administrative act. Considering the nature of opinions, these are equal to advice, guides for action, points of view, and recommendations issued by the administration but that give the administrated the freedom to follow them or not" (Constitutional Court, Judgment C-542, 2015). Although positions do not have the same binding force or character as those from the legislator or the Constitutional Court, they may be used as a guide for CDDBM and for the authorities to apply the law.

party, essential for the functioning of the platform or application, personalized advertising, or website analysis cookies.

Pursuant to the principle of freedom,[29] however, and considering that cookies are used to process data, the current law does demand the prior, informed consent of the data subject before data is collected. Similarly, in the European Union, Article 5(3) of Directive 2002/58/EC (hereinafter, the E-Privacy Directive), as amended by Article 2 of Directive 2009/136/EC,[30] provides that:

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user *is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.* This shall not prevent any technical storage or access *for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*

Thus, the E-Privacy Directive requires the prior, informed consent of the data subject to install cookies on their device and access the stored information. However, unlike Colombia, the European regulation goes beyond the generic requirement of prior, informed consent. To prove this, we must consider several opinions by the Article 29 Working Party, which, although not legally binding, have significant doctrinal value since they were issued by the independent consultation body of the European Union on data protection and privacy matters.

First, as seen in the quote above, the European Union includes reasonable exceptions for consent in the case of certain cookies. Opinion 4/2012 of the Article 29 Working Party expressly provides that a cookie may be exempt from prior, informed consent if it can be clearly identified as an essential prerequisite to carry out (i) the transmission of a communication over an electronic communications network or (ii) the provision of a functionality explicitly requested by the user. In other words,

---

29 See letter Article 4(c) of Law 1581/2012.

30 The E-Privacy Directive has been undergoing further amendments since January 2017, when the Council of the European Union published its proposal to improve and update its guarantees (EC, 2017b).

the cookies necessary for electronic communication or functionality requested by the user are exempt from consent — these are considered "essential cookies." However, the Working Party has clarified that such essentiality must be measured from the user's perspective, not the service provider's (for whom certain behavioral advertising cookies may be "essential" for its marketing strategy).[31] Although there is no regulation on the matter, Opinion 4/2012 of the Article 29 Working Party also provided for a third consent exemption in the case of cookies strictly limited to the anonymized, aggregate statistical purposes of those responsible for analyzing the website (EC, 2012).

Second, European regulations are even stricter regarding consent for behavioral advertising cookies.[32] In Opinion 2/2010, the Article 29 Working Party provided that, in the case of this type of cookie, the consent request must include the following information: (i) who (i.e., which entity) is responsible for the cookie and collecting the related information; (ii) that the cookie will be used to create profiles; (iii) what type of information will be collected to build such profiles; (iv) the fact that the profiles will be used to deliver targeted advertising; (v) the fact that the cookie will enable the user's identification across multiple websites (EC, 2010, p. 4). Clearly, the development of consent provisions for this type of digital tool, and specific exemptions to it, are conspicuously absent from the Colombian personal data protection regime. Consequently, the privacy policies studied here do not require detailed provisions on the advertising and profiling purposes of their data collection. Likewise, essential and non-essential cookies are usually included on the same use authorization and warn that withholding consent may make it impossible to access some of the features of a specific platform.

Lastly, the absence of regulation on the matter results in providers asking for user consent even when cookies (i) collect information required for the service, whether to optimize web browsing, execute a contract (purchase an airplane ticket, make a payment), or sign up and use a

31 Ibid.

32 According to the Article 29 Working Party, behavioral advertising is "based on the observation of the behavior of individuals over time. Behavioral advertising seeks to study the characteristics of this behavior through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests" (EC, 2010, p. 4).

platform (social networking site or subscription service); and (ii) collect anonymized or aggregated information exclusively for statistical purposes by the company responsible for the website.

• *Web crawling*

Web crawling uses computer software to browse the web and index its contents. Although web crawling was not one of the most used data sources by the CDDBMs we studied, its use, in cases such as the Google Search platform, poses important questions for the protection of personal data. Does content indexing imply any type of processing of personal data or, contrarily, does it merely fulfill the role of a simple intermediary between content providers (also responsible for processing the personal data included therein) and content users (also users[33] or recipients of personal data). In other words, the use of web crawling by some CDDBMs makes us wonder if search engine administrators, such as Google Search or Yahoo! Search, may be considered the controllers of personal data when indexing content and, to that extent, if they must (i) ensure the rights to access, rectification, update, or deletion by the subjects of the data processed and (ii) comply with the obligations regarding the quality and update of the data, when requesting consent from the subject, among other times.

In Europe, this question was solved on May 13, 2014, by the Court of Justice of the European Union in its judgment of the case Google Spain, S.L., and Google Inc. *vs.* Spanish Data Protection Agency and Costeja González (Court of Justice, 2014). Here, they discussed if the Spanish Data Protection Agency had acted according to the law by ordering Google Inc. to adopt measures necessary to delete the personal data of Costeja González from its index and to prevent future access to the publications of *La Vanguardia* newspaper that contained them. To solve this issue, the Court of Justice asked

33 Pursuant to letter Article 3(d) of Law 1266/2018, "the user is the natural or legal person who, according to the terms and circumstances set forth in this law, may access the personal information of one or several owners of information provided by the operator or the source, or directly by the owner of such information. The user, to the extent that it has access to third-party personnel, is subject to the compliance with the duties and responsibilities established to ensure the protection of the data owner's rights. In the case that the user also directly provides the information to an operator, he shall be considered as both a user and source, and shall assume the duties and responsibilities of both of them."

> ...in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to Internet users according to a particular order of preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of "processing of … data" used in Article 2(b) of Directive 95/46?

On this matter, it considered that

> …the processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any Internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the Internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the Internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10 eDate Advertising and Others EU:C:2011:685, paragraph 45).

Consequently, it concluded that…

> first, the activity of a search engine consisting in finding information published or placed on the Internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to Internet users according to a particular order of preference *must be classified as "processing of personal data" within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the "controller" in respect of that processing*, within the meaning of Article 2(d). (Italics added)

Because of this judgment, it was established that, in the case of the European Union, the subjects of the data processed through web crawling might demand that Internet operators, among others, delete the results obtained after using describers corresponding to personal data through de-indexation.

In Colombia, the jurisprudential position has been different. Considering that legislation is mute on this matter, the Constitutional Court resolved this issue through Judgment T-040 of 2013. In this judgment, the Court analyzed whether Casa Editorial El Tiempo S.A. and Google Colombia Ltda. had violated the fundamental rights to a good name, honor, and human dignity of Guillermo Martínez Trujillo by failing to delete from their files and records the news article entitled "*Los hombres de la mafia de los Llanos,"* in which the plaintiff was named as a member of a drug cartel. Unlike the Costeja case, in Colombia the Court decided to protect the rights of the plaintiff, and ordered Casa Editorial El Tiempo, and not the search engine, to modify both the title and the contents of the news article. In turn, regarding the responsibility of the search engine, it mentioned the following, which, due to its importance, is transcribed in full:

> Lastly, the Court notes that in this specific case, the responsible of the information issued, and thus of its possible rectification, is the media who collected, analyzed, processed and disclosed the news, that is, Casa Editorial El Tiempo, through its official website. Therefore, said entity would be responsible for the rectification, if applicable. On the contrary, for the Review Chamber, Google Colombia S.A. is not responsible for the news article "*Los hombres de la mafia de los Llanos,"* because, as explained by the company in its response, *Google provides a service for searching the information found online, and it is not the entity that writes or publishes such information, but acts as a simple search engine, which cannot be attributed with any responsibility on the accuracy or impartiality of a respective article, news or column shown in its results.*
>
> *The representative of Google Colombia correctly pointed out that "the search services provider is not responsible for the content of the pages shown as search results,* nor is responsible, as erroneously asserted by the plaintiff, for "maintaining records" of certain information." Regarding the above, Google manages an index that links words to website URL addresses, that is, "it is the file of a large library — the Internet — and the websites which, con-

> tinuing with the example, would be the books of this library, are ordered through it." The information entered into the Internet by the owners of the websites determines the results that Google users will receive in response to their searches, which cover complex subjects or specific interests of each individual.
>
> Therefore, due to the factual elements and to solve this case, *the entity responsible for rectifying, correcting, deleting or complementing the information displayed after a specific search is not Google, but the communication media, writer, journalist etc., who includes and processes the information on the Internet. Without prejudice that, due to different characteristics, there may be cases on which a database that acts as Google may result in any violation to a fundamental right for the information it manages.*[34] (Italics added)

Later, after the ruling of the Court of Justice of the European Union, the Constitutional Court would address this subject again in Judgment T-277 of 2015, discussing whether or not indexing the Internet portal where a news article by Casa Editorial El Tiempo was published affected the fundamental rights of the owner of the personal information included therein, "Gloria." Here, the Court considered that

> … a solution such as that adopted by the Court of Justice of the European Union on the case Costeja v. AEPD, although it represents a mechanism to protect the right to a good name of the person affected by the dissemination of the news article, also implies an unnecessary sacrifice of the Internet neutrality principle and, with it, of the freedom of speech and information.[35]

In contrast, it decided that

> *...in this case the violation of the fundamental right may not be attributable to Google, as it is not responsible for producing the information.* Additionally, we consider it necessary that the reason to not access the deindexation consists in the protection of the principle of net neutrality which, as mentioned above, may only be restricted under exceptional circumstances, as aforementioned.[36]

---

34 Constitutional Court, Judgment T-040, 2013.

35 Constitutional Court, Judgment T-277, 2015.

36 Ibid.

Contrary to the Court of Justice of the European Union, the Constitutional Court decided to order *El Tiempo*, as provider of the contested content, to prevent its appearance in search engine results by using technical tools such as "robots.txt" and "metatags."

Three things must be noted regarding these two judicial rulings. First, although neither of the two judgments declared the responsibility of the search engine, the first left the possibility of future responsibility open:

> …the entity responsible for rectifying, correcting, deleting or complementing the information displayed after a specific search is not Google, but the communication media, writer, journalist etc., who includes and processes the information on the Internet. *Without prejudice that, due to different characteristics, there may be cases on which a database that acts as Google may result in any violation to a fundamental right for the information it manages.*[37] (Italics added).

Second, although both judgments mention that the media is responsible for the violation of rights, the orders adopted by the court are very different. While in the case "*Los hombres de la mafia de los Llanos*" the court ordered the newspaper to amend the news article, in the case of "Gloria" the court decided to order the use of certain technological tools to "detag" the disputed content so that it would not be detected by the search engine.

Finally, in these two judgments, the Court considered that, as this was journalistic information, the right in dispute was not related to the right to the protection of personal data[38] but rather to the rights to honor and a good name. Although the decisions adopted released the search engine from responsibility, they did not consider whether its operator was processing personal data. This is fundamental, as it shows that, unlike Europe, the nature of personal data regarding entities that carry out web

---

37 Constitutional Court, Judgment T-040, 2013.

38 For example, Judgment T-040 of 2013 provided that: "The fundamental *habeas data* right mentioned by the plaintiff is not applicable in this case, considering that the discussion focuses on the journalistic information disseminated on a communication media in the exercise of freedom of speech, and on its rectification, not on information contained in a database or files regulated by the Statutory Law analyzed by this Court on Judgment C-748 of 2011" (Constitutional Court, Judgment T-040, 2013).

crawling is still to be defined in Colombia, whether through law or a new ruling by the Court.

• *Data commercialization*

The only legal provision in Colombia that expressly refers to the commercialization of personal data is contained in article 269F of the Criminal Code, on the felony of personal data violation:

> Who, *without being authorized to do so*, for their own 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 for forty-eight (48) to ninety-six (96) months, and a fine of between 100 to 1000 monthly legal minimum wages. (Italics added)

Considering that the felony consists of selling personal data contained in archives, files, databases, or similar means *without being authorized to do so*, we infer that selling said information is legal in Colombia *with* authorization. But, when is someone authorized? Based on the principles of personal freedom[39] and personal data protection, we assume that, as with all other personal data processing, a person is authorized to commercialize data only when it has obtained the prior, express, informed consent from the data subject, or with a legal or judicial mandate releasing the entity from obtaining such consent. It seems that authorization by the subject — or a legal or judicial mandate — are the only limitations to data commercialization that exist in Colombia. However, note that in Chapter 2 of this document we presented data commercialization not only as a type of processing, but also as a *purpose*. Therefore, if it is a *purpose*, the commercialization of data — mainly selling information to data brokers — would also be conditioned by the principle of purpose set forth in letter Article 4(b) of the aforementioned law: "the processing must be the result of a legitimate purpose pursuant to the Constitution and the Law, which must be notified to the Subject."

According to the Constitution and Colombian law, is the commercialization of personal data legitimate? In principle, regarding data processing performed by private companies, it is, because the principle of legality — everything that is not forbidden is allowed — is applicable to

39 See letter Article 4(c) of Law 1581/2012.

private entities. Therefore, as there is no provision that forbids the sale of data with authorization from the subject, it seems that this activity is legal. Additionally, it seems to be the posture of all the CDDBMs we studied that data is part of the company's assets; as such, it may be sold or assigned should the company be sold or merged. However, this incipient regulation of data commercialization or data brokering contrasts with California's CCPA, which expressly allows consumers to forbid the sale of their personal information by a company (defined in the law 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 quality of the good or service they offer,[40] except "if that difference [in price or quality] is reasonably related to the value provided to the consumer by the consumer's data."[41] 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) affirmatively authorize it (referred to in the law as the right to opt in).[42] Additionally, the incipient Colombian regulation ignores the obvious risks derived from the sale of personal data. According to the Article 29 Working Party, a data broker is a company that

> …collects data from different public and private sources, either on behalf of its clients or for its own purposes. […] compiles the data to develop profiles on the individuals and places them into segments. It sells this information to companies who wish to improve the targeting of their goods and services. […] carries out profiling by placing a person into a certain category according to their interests. (EC, 2017a, p. 8)

This definition is relevant because, as recognized by the Constitutional Court of Colombia in Judgment T-414 of 1992,

> …the "data profile" of an individual becomes, therefore, a sort of "virtual person," over which several actions that could have repercussions on the real person may be performed. From sending unsolicited advertisements, to coercion or social "ostracism," as in this case. A "good" use of data banks will allow the identification of population profiles from different perspectives,

40 See Section 1798.120(a) of the CCPA.

41 See Section 1798.125(a)(2) of the CCPA.

42 See Section 1798.120(c) of the CCPA.

> which constitutes an obvious social control hazard from those who hold "computing power," not only against the freedom of individuals, but against the freedom of broader social sectors.[43]

Likewise, the Article 29 Working Party has recognized that profiling poses risks for the rights and freedoms of individuals, to the extent that

> …these processes can be opaque. Individuals might not know that they are being profiled or understand what is involved. Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustified discrimination. (EC, 2017a, pp. 5–6)

Some examples of the perpetuation of existing stereotypes and the social segregation that profiling may cause can be found in cases such as big data policing (Ferguson, 2017), where profiling is used by police authorities to predict crime based on determined profiles built from data whose racial neutrality has been seriously questioned and which may perpetuate discriminatory stereotypes. Another example is the use of profiling to predict the performance and potential of job candidates, whose assessment criteria might be biased by sensitive personal data such as gender or socioeconomic status. Thus, if data brokers can purchase personal data to create profiles of the data owners, and such profiles constitute a clear hazard for social control, discrimination, and restriction of freedoms, we cannot understand why these, as well as the sale of the data that enables them, may be freely performed by the CDDBMs who collect data in Colombia without any specific regulation on the matter.

In contrast, in section 60, the GDPR has attempted to promote *transparency* in profiling: "Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling." Likewise, considering that the profiling process implies the creation of "new" (inferred) information not directly provided by the data subject, article 14 of the GDPR establishes particular transparency requirements when

43 Constitutional Court, Judgment T-414, 1992.

the data was not "voluntarily" provided by the data subject. From this, it is worth noting the requirement to inform the data subject of the existence of this information held by the controller "within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed."[44]

Likewise, when interpreting article 5(1)(a) of the GDPR in the case of profiling, the Article 29 Working Party mentioned that "profiling may be unfair and create discrimination, for example by denying people access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products" (EC, 2017a, p. 10). Therefore, the GDPR also intended to promote the *fair nature* of data processing, including profiling.

• *Personalized content*

The offer of personalized content (including advertising) is one of the purposes of personal data processing performed by the CDDBMs we studied. However, the personal data protection regime currently in force in Colombia does not regulate the matter beyond the general requirement that be (i) legitimate pursuant to the Constitution and the Law, and (ii) informed to the data subject at the time of collection of the personal data. Unfortunately, the limited scope of this regulation does not consider the multiple particularities of allowing the use of personal data to provide contents and, particularly, personalized advertising. First, it ignores that personalized advertising is based on profiling,[45] a practice which, as shown above, poses significant risks to the rights and freedoms of individuals. Second, it dismisses the fact that personalized advertising is not always the same, as it might be more or less invasive of the privacy of individuals. On the one hand, there is *contextual advertisement* "selected based on the content currently being viewed by the data subject"; on the other hand, there is *segmented advertisement* "selected based on known characteristics of the data subject (age, sex, location, etc.), which the data subject

---

44 Article 14(3)(a) of the GDPR.

45 Note that targeted advertisement is possible through "basic Internet technology [which] allows advertising network providers to track data subjects across different websites and over time. Information gathered on the surfing behaviour of data subjects is analysed in order to build extensive profiles about data subjects' interests. Such profiles can be used to provide data subjects with tailored advertising" (EC, 2010).

has provided at the sign up or registration stage" (EC, 2010, p. 5). Most invasive is *behavioral advertising*, which consists of the

> … observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests. (EC, 2010, p. 4)

Third, the practically non-existent regulation on the matter underestimates the fact that more than one actor is involved in behavioral advertising, not only the CDDBMs who provide the ad space, but also advertisers and ad network providers. Thus, while CDDBMs reserve ad space on their websites to show an ad, they assign the rest of the advertisement process to one or more ad network providers. In turn, they install cookies on the websites of all their clients to monitor users and "track" their behavior. In this way, they build a profile of the visitor that will then be used to recommend to ad providers which ad spaces to promote their products (EC, 2010, p. 4). Therefore, as recognized by the European Union, in this type of advertisement "the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected."[46]

Thus, the purpose of the provision of personalized content (particularly behavioral advertising) must be expressly regulated to prevent both the illegal invasion of user/client privacy, and their total ignorance regarding a data-based activity of which various actors take advantage.

• *Automated decision-making*

Automated decision-making has been defined as "the ability to make decisions by technological means without human involvement" (EC, 2017a, p. 8). According to the principle of purpose established under Law 1581/2012, "the processing must be the result of a legitimate purpose pursuant to the Constitution and the Law, which must be notified to the subject." In the case that automated decision-making is a purpose of the processing, it is understood that it must be (i) legitimate pursuant to the constitution and the law, and (ii) be notified to the data subject.

46 Section 58 of GDPR.

Additionally, article 5 of the regulatory decree of Law 1581/2012 demands the purpose to be specific.[47] As with the provision of personalized content, however, these three conditions leave out many other fundamental requirements to prevent decisions without human involvement from compromising the rights of the data subjects involved. For such events, it is worth quoting article 22 of the GDPR, Automated Individual Decision-Making, Including Profiling:

> 1. *The 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.*
>
> 2. Paragraph 1 shall not apply if the decision:
>
> a) is *necessary for entering into, or performance of, a contract* between the data subject and a data controller;
>
> b) is authorized by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
>
> c) is based on the data subject's explicit consent.
>
> 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least *the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*
>
> 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Thus, unlike Colombia, the European Union has taken measures to prevent the possible risks from automated decisions. Therefore, the GDPR

47 According to article 5 of Decree 1377/2013, "the Data Controller shall adopt procedures to request, no later than at the time of the data collection, the authorization of the Data Subject to process the data and inform what personal data will be collected, as well as the specific purposes of the processing for which the consent is being obtained."

not only gave the data subject the ability to opt out from said processing purpose if it may produce legal effects for him or her[48] or other significant effects.[49] Additionally, should the purpose be accepted, the data subject has the right to (i) obtain human intervention from the controller, (ii) express his or her point of view, and (iii) contest the decision. Additionally, the GDPR expressly forbade automated decision-making based on sensitive data, except when this processing has been expressly authorized by the data subject, or is necessary for the public interest, in which case suitable safeguards must be adopted.

These conditions, although limited,[50] aim to *provide transparency* to automated decisions to give the data subject more control, in accord with the Guiding Principles on Business and Human Rights, which include transparency measures. Particularly, recommendation 21 provides that:

> … In order to account for how they address their human rights impacts, *business enterprises should be prepared to communicate this externally, particularly when concerns are raised by or on behalf of affected stakeholders.* Business enterprises whose operations or operating contexts pose risks of severe human rights impacts should report formally on how they address them. In all instances, communications should: a) Be of a form and frequency *that reflect an enterprise's human rights impacts and that are accessible to its intended audiences*; b) Provide information that is sufficient to evaluate the adequacy of an enterprise's response to the particular human rights impact involved; c) In turn not pose risks to affected stakeholders, personnel or to legitimate requirements of commercial confidentiality.

Likewise, they seem to coincide with the provisions of the United Nations Resolution on the Right to Privacy in the Digital Age A/C.3/71/L.39, which exhorts countries and business:

---

48 According to the Article 29 Working Party, this implies an affectation to the legal rights, such as the cancellation of a contract, the entitlement to a particular social benefit, or the admission to a country (EC, 2017a).

49 According to the Article 29 Working Party, this implies that the decision has the potential to: (i) "significantly affect the circumstances, behaviour or choices of the individuals concerned"; (ii) "have a prolonged or permanent impact on the data subject"; or (iii) "at its most extreme, lead to the exclusion or discrimination of individuals" (EC, 2017a, p. 21).

50 It is still not clear what a "significant" affectation implies, which may reduce the effectiveness of these conditions.

> (i) To consider appropriate measures that would enable business enterprises to adopt voluntary transparency measures with regard to arbitrary or unlawful requests by State authorities for access to private user data and information; […] l) To ensure that decisions based on automated processing that significantly affect the rights of an individual are transparent and have no discriminatory impact.

What is inadequately regulated

• *Sharing personal data for academic research*

Like the privacy policies of the CDDBMs we studied, the Colombian legal regime expressly considers the possibility that the controller may share personal data with third parties for academic research purposes (particularly historical, statistical, or scientific research). In fact, it includes this situation as one of the cases in which the authorization of the data subject is not necessary. Thus, letter article 10(d) of Law 1581/2012 provides that "the authorization of the Data Subject shall not be necessary in the case of: d) processing of data authorized by the law for historical, statistical or scientific purposes." Furthermore, it includes this situation as one of the cases under which processing sensitive personal data is allowed, although it mentions "in this case, measures aimed at suppressing the identity of the Data Subjects shall be adopted."[51]

In our opinion, the requirement to anonymize sensitive data is insufficient in the face of the digital age since such a large volume of data makes it possible that the subject may be eventually re-identified, which the European Union certainly realizes. Even before the GDPR, the EU demanded that the data controller must ensure that the measures used to anonymize (or aggregate or pseudonymize) should ensure the following:[52] (i) rule out the use of the data in support of measures or decisions regarding any particular individual;[53] and (ii) be accompanied by a compatibility assessment that analyzes, in each specific case, if the processing for research

---

51 See Article 6(e) of Law 1581/2012.

52 Defined in Article 4(5) of the GDPR as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

53 See Section 29 of Directive 95/46/EC.

purposes is compatible with the purpose for which the personal data were initially collected. For this purpose, the Article 29 Working Party (EC, 2013) established four criteria to be considered, later included in Article 6 number 4 of the GDPR: (i) any link between the purposes for which the personal data have been collected and the research purposes; (ii) the *context* in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (iii) the *nature* of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed; (iv) the *possible consequences* of the intended further processing for data subjects.

Unlike Colombia, the European Union has established that personal data may be processed — always anonymously — for research purposes, provided it can be demonstrated that the research purpose is related to the initial purposes for which the data were collected; that the relationship between the data subjects and controllers is not unbalanced nor implies any type of coercion; that no special categories of personal data are involved; and that the corresponding academic research will not have consequences on the lives of the subjects whose data will be processed. Clearly, these safeguards may not be deduced from the Colombian regulations, whose existence would limit the possibility of sharing sensitive personal data for academic research even more in order to ensure the protection of the rights of the subjects, but without obstructing the progress of science.

• *Prior, express, informed consent*

Considering that the provisions of Law 1581/2012 do not expressly refer to data commercialization, profiling, or automated decision-making, these could be performed once the data subject provides their prior, express, informed consent, which must be obtained but may be subject to further consultation.[54] In practice, in Colombia this consent is given by accepting a set of privacy policies (legally named "information processing policies"), which, by law, must be published by the CDDBMs and which (i) due to their length are read by few people, (ii) due to their complexity are understood by few people, and (iii) due to their vagueness, it is difficult to measure the implications of accepting them. Additionally, these policies do not give the data subject the freedom to choose the processing and purposes they wish to authorize as (i) they present the information as

54 See Article 9 of Law 1581/2012.

a block, without allowing for excluding some processing or purposes and accepting others, and (ii) they make the provision of service conditional on the complete acceptance of such policies. In some cases, however, the user does not face such privacy policies, as many CDDBMs assume that their presence on the app or platform is, as provided in the Regulatory Decree of Law 1581/2012, an "unequivocal [...] conduct [...] of the Data Subject that allows reasonably concluding that he or she granted said authorization."[55]

Clearly, this diagnosis questions the utility of prior, express, informed consent to protect personal data *effectively*.[56] Consequently, in response, the concept of "consent" initially included in EU Directive 95/46/CE and the E-Privacy Directive has had to evolve. Although the definition of consent in the GDPR was very similar,[57] sections 32, 42, and 43, and article 7 included additional guidelines to enforce it.[58] Article 7(4) clarified that

---

55 Article 7 of Decree 1377/2013. Unfortunately, when we asked the Superintendence of Industry and Commerce about the legality of this practice, the head of the Legal Counsel Office responded: "This Legal Counsel Office has no competence to determine whether a personal data subject granted his prior and express consent by using a website for the mere fact that the website contains the terms and conditions of use, data policy, etc., as this must be analyzed by the Directorate for Investigations on the Protection of Personal Data of this entity as part of an administrative investigation" (SIC, 2016b).

56 In this regard, see the statements by Magistrate Ciro Angarita Barón on the effective protection of the rights ordered by the Constitution; for example, Constitutional Court, Judgment T-406, 1992.

57 Thus, while Article 2(h) of Directive 95/46/CE defined consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed," number 11 of article 4 of the GDPR defined consent as "any freely given, specific, informed and *unambiguous* indication of the data subject's wishes by which he or she, *by a statement or by a clear affirmative action,* signifies agreement to the processing of personal data relating to him or her" (italics added).

58 Note that these new guidelines have not been an obstacle to continue abusing the figure of consent. Thus, on the same day as the effective date of the GDPR (May 25, 2018), the Noyb organization presented four complaints against Google (Android), Facebook, WhatsApp, and Instagram for "forced consent," as their "consent check boxes" were threatening the user that the service could no longer be used if they did not give their consent. Likewise, on June 26, 2018, the Norwegian Consumer Council published a report on the manipulation of consent through the design of interfaces (Noyb, 2018; Forbrukerradet, 2018).

> …when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, *is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*. (Italics added)

In this way, it excluded the validity of cases such as that mentioned by the Article 29 Working Party in Example No. 1 of the working document "Guidelines on consent under Regulation 2016/679." This example describes the case of a mobile app for photo editing that (i) asks users to have their GPS localization activated to use its services; (ii) tells users that it will use the data collected for advertisement purposes. Considering that neither geo-localization nor online behavioral advertising are necessary for the provision of the photo editing service, the Working Party considers that this case violates the provisions of article 7 number 4 mentioned above, since "users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given" (EC, 2018, p. 6). In turn, section 43 of the GDPR provides that

> …consent is presumed not to be freely given *if it does not allow separate consent to be given to different personal data processing operations despite* it being appropriate in the individual case, or *if the performance of a contract, including the provision of a service, is dependent on the consent* despite such consent not being necessary for such performance. (Italics added)

Similarly, the relevant parts of section 32 provided that "consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them." In this way, the GDPR makes it clear that both the block presentation of the terms and the conditionality of a service are indications that consent has not been freely given. Therefore, it requires both the "granularity" and the unconditionality of the terms and conditions and the privacy policies presented to request the user's consent.

Additionally, the relevant parts of section 42 of the GDPR provide that "in accordance with Council Directive 93/13/EEC (1) a declaration of consent pre-formulated by the controller should be provided *in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms"* (italics added). As a complement, the Article 29 Working Party mentioned, "if consent is to be given by electronic means,

the request *must be clear and concise*. *Layered and granular information* can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand." Thus, these instruments suggest practical tools to comply with the obligation, non-existent in Colombia, of presenting the information on the processing and purposes in a clear, precise, concise, and intelligible form to the target audience.

Lastly, unlike article 2(h) of Directive 95/46/CE — currently revoked — article 4(11) of the GDPR refers to an "*unambiguous* indication of the data subject's wishes by which he or she, *by a statement or by a clear affirmative action*, signifies agreement to the processing of personal data relating to him or her" (italics added). As said by the Article 29 Working Party, the direct consequence of this provision is that "the use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice" (EC, 2018, p. 16). Likewise, "the GDPR does not allow controllers to offer […] opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes')" (EC, 2018, p. 16). This shows that the conditions currently regulating prior, express, informed consent in Colombia leave vast room for improvement before they can be considered a true safeguard of the right to the protection of personal data.

Territorial application of personal data protection law

In addition to establishing whether the contents of Law 1581/2012 are sufficient to hold CDDBMs accountable in the digital age, we must also establish whether the scope of the territorial application of the law covers them. According to Article 2 of Law 1581/2012, the Colombian data protection law is applicable to the processing of personal data (i) performed in Colombian territory or (ii) when Colombian law applies to the controller or processor not constituted in Colombian territory pursuant to international regulations or treaties.

Under a literal interpretation of this article, one could understand that, unless Colombian law applies to them pursuant to international regulations or treaties, Law 1581/2012 is not applicable to CDDBMs *not domiciled in Colombia,* as their processing takes place wherever their

facilities (and servers) are located, not in Colombia. In fact, this was the initial consideration of the Deputy Superintendence for the Protection of Personal Data (SIC, 2014a) acting in its capacity under Opinion 14-218349-00003-0000, dated November 24, 2014, regarding whether Colombian personal data protection law was applicable to social networking sites such as Facebook. Here, the SIC considered that

> …the processing of personal data registered on social networking sites is not within the scope of competences of Law 1581/2012, as the collection, use, circulation, storage or deletion of personal data *does not take place in Colombian territory, as the social networking sites have no domicile in Colombia.* (Italics added)

Apparently inspired by article 4(1)(c)[59] of Directive 95/46/CE, however, the Superintendence of Industry and Commerce (SIC, 2016a) changed its stance on the matter in Opinion 14-218349-4-0, dated March 3, 2016, by mentioning that:

> Undoubtedly, the aforementioned legal provision extends the scope of application of the personal data protection statutory law to countless scenarios of processing of personal information in Colombia, e.g., The processing of personal data carried out by the providers of social media services *domiciled outside of the country through "means" located in Colombian territory.* (Italics added)

Therefore, from this moment, it was clear that (i) Law 1581/2012 applies to controllers or processors domiciled in Colombia, and (ii) its scope of application also extends to controllers or processors not

---

59 According to which:
Article 4. National law applicable.
1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: [...]
c) the controller is not established on Community territory and, *for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State*, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

domiciled in Colombian territory when a) the Colombian law applies to them pursuant to international regulations or treaties or b) the processing of the relevant personal data is carried out through "means" located in Colombian territory. Although the SIC did not provide so, it has been understood that by "means" the data protection authority referred to the cookies stored in the user's computer (located in Colombian territory) when they visit a website.

Is this scope enough to hold the CDDBMs that collect data in Colombia accountable? In the case of companies domiciled in Colombia, such as most "startups" and "established companies" in our study, yes it is. The situation of large Internet companies and most "intermediate companies" is different, however, as most are not domiciled in Colombia. If we start from the assumption that all these companies collect data through cookies, we can conclude that collection processing at least is covered under Colombian law. As shown in Chapter 2 of this document, however, it is clear that web tracking is not the only data source used by these companies. Furthermore, what would happen with any other operation or set of operations that said companies decide to carry out on these personal data, such as their storage, use, circulation, or crossing with other data? In the event that these other processes are carried out through "means" located in a different territory, they would be outside of the scope of territorial application of the Colombian law.

Therefore, 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 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 depend on the location of the personal data subjects being processed. The scope of territorial application was extended to all kinds of processing made on the personal data of the "data subjects who are in the Union," that is, the "identifiable natural person[s]"[60] who are data subjects.[61]

---

60 Article 4(1) of the GDPR.

61 Thus, pursuant to Article 3(2) of the GDPR, said regulation is applicable to the processing of personal data of *data subjects who are in the Union by a controller or processor who is not domiciled therein*. However, the applica-

Additionally, both Article 2 of Law 1581/2012, and its interpretation by the Superintendence, fall short in defining what happens when the controller or processor is not domiciled in Colombian territory but has an establishment or any other type of representation therein (affiliate, branch, etc.). Although the Colombian constitutional jurisdiction already had to resolve this matter through jurisprudential means[62] to define the passive legitimacy of the cause in several cases, the fact is that having a legal provision such as article 4(1)(a) of the revoked Directive 95/46/CE would provide more legal security. In this case, the Member States of the European Union had to apply the Directive to all processing of personal data "carried out in the context of the activities of an establishment of the controller on the territory of the Member State." By interpreting this provision in the case of Google Spain, S.L., and Google Inc. *vs.* the Spanish Data Protection Agency and Costeja González, the Court of Justice of the European Union mentioned that

> Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, *when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.*

It was established that the European data protection regulation was also applicable to data processors not domiciled in the European Union when it had a branch or subsidiary established in its territory, whose activities were related to the processing of personal data carried out by its parent company. Thus, although in this case the manager of Google Search was Google Inc., it was clear that the activities to promote and sell advertising space offered in Spain by Google Spain were related to the processing of personal data carried out in Google Search, meaning that Directive 95/46/CE was applicable to said processing. Based on this interpretation, the article related to the territorial scope of the GDPR was

bility is conditioned to the processing activities related to "(i) *the offering of goods or service*s, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (ii) *the monitoring of their behaviour* as far as their behaviour takes place within the Union."

62 See Constitutional Court, Judgment T-063A, 2017.

much more explicit on the matter. Article 3(1) provided that said regulation is applicable to the processing of personal information "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"* (italics added).

Capacities of the competent authorities

Capacities to regulate, monitor, control, and sanction CDDBMs

Colombia does have a personal data protection authority, which places it in a better position than countries such as the United States, where this capacity has been assumed — *de facto* — by the Federal Trade Commission (FTC) through consumer protection. Particularly, regarding the application of Section 15 U.S.C. Sec 45(a)(1) of the Federal Trade Commission Act,[63] the FTC has protected digital consumers from certain unfair data collection policies. For example, in March 2016 it sent warning letters to app developers who allowed third parties to install a piece of software (audio beacons) that can monitor a device's microphone to listen for audio signals embedded in television advertisements into their applications in order to monitor the television use of consumers for targeted advertising purposes (FTC, 2016). Additionally, the FTC makes suggestions regarding the degree to which companies must protect user data. Thus, it works closely with groups such as the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA) to encourage the "industry to provide consumers with basic privacy protections, including transparency and consumer control, reasonable security and limited retention for consumer data, and affirmative express consent for the use of sensitive data" (FTC, 2017, p. 1). The guidelines established by the FTC are not legally binding, however, and membership to the NAI and DAA are entirely voluntarily, so companies are not obliged to adhere to these guidelines.

In contrast, in its capacity as personal data protection authority in Colombia, the Office for the Deputy Superintendence for the Protection of Personal Data, and its Directorate for Investigations on Personal Data Protection, carry out various duties. It has *regulatory duties*, mainly aimed at the following:

---

63 Pursuant to which "unfair methods of competition in or affecting commerce [...] are hereby declared unlawful."

1. "promoting and disseminating the rights of people regarding the processing of personal data, and shall implement pedagogical campaigns to train and inform citizens on the exercise and enforcement of the fundamental right to data protection"[64]
2. "give instructions on the measures and procedures required by the data controllers and processors to adhere to the provisions set forth in the law"[65]
3. "issue relevant statements regarding the international transfer of data"[66]
4. "suggest or recommend corrective adjustments or amendments to the regulations pursuant to the technological, informatics and communications evolution"[67]

Additionally, it has *control and monitoring duties*, such as these:

1. "ensure the compliance with the law in personal data protection matters"[68]
2. "order the temporary blocking of data when, upon request and considering the evidence contributed by the data subject, there is an actual risk of violation of his or her fundamental rights, and said blockage is required to protect them while a definitive decision is adopted"[69]
3. "ask the data controllers and processors to provide the information required for the effective exercise of its duties,"[70] and, particularly, to demonstrate, pursuant to the principle of responsibility, "that they have implemented adequate and effective measures to comply with the obligations set forth in Law 1581/2012"[71] and its Regulatory Decree
4. "manage the National Public Data Base Registry and issue the orders and actions required for its administration and operation"[72]

---

64 Article 21(e) of Law 1581/2012.

65 Ibid. Also, refer to articles 11 and 27 of Decree 1377/2013.

66 Article 21(g) of Law 1581/2012. Also, refer to Article 16(5) Decree 4886/2011.

67 Ibid., paragraph (i).

68 Ibid., paragraph (a).

69 Ibid., paragraph (c). Also, refer to article 16(4) of Decree 4886/2011.

70 Ibid., paragraph (f).

71 Article 26 of Decree 1377/2013.

72 Article 21(h) of Law 1581/2012.

Finally, it has *punitive duties*, including the following:

1. "conduct the relevant investigations, pursuant to law or at the request of a party and, as a result thereof, order the measures required to enforce the habeas data right. For such effects, anytime this right is violated, it may order the access and provision of the data, and their rectification, update or elimination"[73]
2. "require the collaboration of international or foreign entities whenever the rights of data subjects outside of the Colombian territory are being violated as a result of the international collection of personal data"[74]

Regarding the exercise of these duties, the Deputy Superintendence for the Protection of Personal Data should have at least two strengths. First, the human talent of the office must have the expertise (i) to recommend adjustments, corrections, or adaptation to the regulations according to the technological, computational, and communications evolution, and (ii) to ensure that operators and sources have appropriate security systems and technical conditions. In order to do this, it must have officers with appropriate skills to understand the operation of data exploitation, such as systems engineering, mathematics, statistics, machine learning, and data science. Similarly, to be able to ensure the human right of the protection of personal data in each specific case — resolving the tensions it may have with others, such as the right to access public information or to freedom of speech — a team with a human rights approach, and not an exclusively commercial approach, is required.

Second, the Deputy Superintendence for the Protection of Personal Data must cultivate as much autonomy and independence as possible before the companies it must regulate, control, monitor, and penalize, including the CDDBMs. Thus, although we agree with the utility and complementary nature of self-regulation, we also believe in the virtues of a purely state — or even international — regulation such as that developed by the GDPR. Therefore, in the case of the Deputy Superintendence for the Protection of Personal Data, we emphasize that a close relationship with the regulated parties without due supervision is problematic, as it poses risks to its independence and impartiality when exercising its monitoring, control, and penalizing duties.

---

73 Ibid., paragraph (b).

74 Ibid., paragraph (j). Also, refer to Article 16(6) of Decree 4886/2011.

Competence regarding CDDBMs

It seems clear that, in the case of Colombia, the scope of application of Law 1581/2012 extends to data controllers or processors not incorporated in Colombian territory only when (i) Colombian law applies to them pursuant to international standards or treaties, or (ii) the relevant processing of personal data is carried out through "means" located in Colombian territory. But how is this scope implemented in practice if the data controller or processor is not domiciled in Colombia, as in the case of Google LLC, Deezer SA, or the Alibaba Group? How do the competent authorities — whether the Superintendence of Industry and Commerce or the judges of the Republic — call on these companies to be accountable? In the end, it is a matter of passive legitimation of who is to be held accountable in personal data processing matters before the data protection authority and the Colombian judges.

In the case of the Deputy Superintendence for the Protection of Personal Data, its actions regarding the CDDBMs we studied do not give much information about this legal problem. The only companies in our sample that have been subjected to penalties by the data protection authority are "established companies" usually domiciled in Colombia. Upon reviewing the sanctions database of the Deputy Superintendence for the Protection of Personal Data (SIC, 2018b), which includes sanctions imposed between 2014 and 2018 for improper processing of personal data, we confirmed that Almacenes Éxito S.A. (2), Telmex Colombia S.A. (1), and Grupo Aval Acciones y Valores S.A. (through Banco de Occidente S.A.) (1) are the only companies that have been sanctioned.

Almacenes Éxito S.A. was initially sanctioned on May 30, 2014 (SIC, 2014a), for failing to correct the name of one of its clients, which was badly incorporated in the database of the customer loyalty program "*Superclientes Carulla,*" and failing to inform her where to find the personal data processing policy. Likewise, on June 25, 2018 (SIC, 2018a), the company was sanctioned again for failing to delete the email address of one of its clients and for continuing to send her emails with advertising content, despite her wishes. Banco de Occidente S.A., part of Grupo Aval Acciones y Valores S.A., was sanctioned on December 13, 2016 (SIC, 2016c), for failing to have the corresponding evidence of the consent given by its clients to (i) use their email address to send advertisement emails regarding a credit funding scheme, or (ii) massively disclose said email addresses to other clients. Telmex Colombia S.A. was sanctioned on November 30,

2017 (SIC, 2017), for failing to delete the email address of a person who was not a client of the company from its database, thus allowing him to continue receiving billing emails for an account not owned by him.

Although these cases are useful to get an idea of the type of problems addressed by the Superintendence in the framework of the digital age (mainly related to emails and digital advertisements), they do not allow for establishing the position of the data protection authority regarding the passive legitimation of the data controller called upon to be accountable in our country while not being domiciled in Colombia.

The exercise of its duties set forth in article 21(j) of Law 1581/2012, although sparse, seems to show the intention of our personal data protection authority to hold CDDBMs not domiciled in Colombia accountable through international cooperation. According to this paragraph, the duties of the SIC include "asking for the collaboration of international or foreign entities when the rights of data subjects are affected outside of the Colombian territory due to, inter alia, the international collection of personal data." Likewise, article 16(6) of Decree 4886/2011 includes the same wording as part of the duties of the Office of the Deputy Superintendent for the Protection of Personal Data. In exercising this duty, at the time of Deputy Superintendent José Alejandro Bermúdez, various companies in Colombia whose personal data processing had the potential of affecting Spanish citizens were inspected.[75] Thus, although we still do not have evidence of cases of cooperation in inspecting foreign CDDBMs with the potential to affect Colombian citizens, this seems to be an option that the SIC has explored.

Regarding the Constitutional Court, in its capacity to judge the effective protection of personal data, its position regarding the passive legitimation of CDDBMs with no domicile in Colombia has been more explicit. Specifically, the Court has had to face the problem of the passive legitimation of Google Inc. (currently Google LLC)[76] on three occasions. Unfortunately, in none of these cases did the court analyze the violation of the right to the protection of personal data, whether because the cases

---

75 This information was obtained thanks to the participation of the former Deputy Superintendent José Alejandro Bermudez in the focus group carried out on November 20, 2018, upon publication of this document in Spanish. See Annex 3 for the list of attendees.

76 In September 2017, Google became a limited liability company (LLC) and stopped being a corporation.

were about journalistic information (to which Law 1581/2012 does not apply, but its governing principles do) or because it decided, inexplicably and ultimately erroneously, that consumer rights were those at stake. Despite this lost opportunity, the content of these three judgments continues to be useful to analyze how this type of company, with no domicile in Colombia, has been held accountable in the country.

The first case, already mentioned above, took place in 2013. In this case, a man filed a writ for the protection of fundamental rights against Google Colombia Ltda. and Casa Editorial El Tiempo S.A., requesting that, in order to protect his fundamental rights, the defending entities were ordered to delete from the records of the newspaper and from Google Search the news article entitled "*Los hombres de la mafia en los Llanos,*" which mentioned him. Here, Google Colombia Ltda. replied to the claim with the following arguments:

> Google Colombia has a commercial purpose –the direct or indirect sale, distribution, commercialization and development of hardware and software products and services, Internet related products and services and Internet advertisement, or through any other means–; therefore, Google Colombia is not the entity responsible for the charges presented by the plaintiff, as it is not the entity that manages Google Inc.'s search service[77]
>
> the provider of search services is not responsible for the contents of the websites shown as search results and is not responsible for –maintaining records of certain information', as mistakenly stated by the plaintiff–.[78]

This was the first time the difference between the corporate purpose of Google Colombia Ltda. and Google Inc., with the latter being the search service provider and, to that extent, the alleged processor of the data, was used. Unfortunately, upon reviewing the passive legitimacy of the writ for the protection of fundamental rights, the Constitutional Court only referred to the second argument presented by the company, on which the controller of the information issued, and thus the party responsible for its possible rectification, was the communication media who collected, analyzed, processed, and disseminated the news article, that is,

77 Constitutional Court, Judgment T-040, 2013.

78 Ibid.

Casa Editorial El Tiempo through its official website. Accordingly, the Court considered that

> Google Colombia S.A. is not responsible for the news article "*Los hombres de la mafia de los Llanos,*" because, as explained by the company in its response, Google provides a service for searching the information found online, and it is not the entity writing or publishing such information, but acts as a simple search engine, which cannot be attributed with any responsibility on the accuracy or impartiality of a respective article, news or column shown in its results.[79]

In this way, the court avoided addressing the problem of Google Inc. as a legal person in Colombia by generally referring to "Google."

Later, this legal problem would arise again in the case, also described above, about a woman the court named "Gloria" who filed a writ for the protection of fundamental rights against Casa Editorial El Tiempo. Her writ asked that a news article informing on the alleged participation of the plaintiff in human trafficking be removed from all available search engines, specifically Google.com. Although the defendants did not include Google Colombia Ltda., the First Review Chamber of the Constitutional Court ordered its inclusion in the proceedings to record its statement on the facts and claims of the constitutional action. Similarly to the preceding case, in responding to the claim, Google Colombia Ltda. mentioned that it "lacks passive legitimation since this is not a branch company and does not legally represent Google Inc.; therefore, an order cannot be given to Google Inc. and it cannot be executed by Google Colombia, as the latter has no control over the actions of its parent company."[80] It states that the "management and control of the Google search engine and the Internet domains www.google.com and www.google.com.co correspond to Google Inc., a company incorporated in the United States of America and domiciled therein." Likewise, it reiterated that the only company responsible for the publication is Casa Editorial El Tiempo, owner of the website that shows said content, and who may decide what part of the content may be indexed by the search engines.

Once again, the Constitutional Court did not refer to the legal person of Google Inc. in Colombia, instead stating that "ordering Google.com

---

79 Ibid.

80 Constitutional Court, Judgment T-277, 2015.

search engine to block the website of a communication media that informs the arrest and criminal investigation against 'Gloria' from its search results would imply the implementation of a prior control measure that violates the principle of neutrality."[81] In this way, the court ignored the fact that it would be procedurally impossible to order the controller of the search engine to block certain results, as the legal entity had not been included in the proceedings.

A third case would be judged in February 2017. This time, a man filed a writ for the protection of fundamental rights against Google Inc. and Google Colombia Ltda. to receive the protection of his fundamental rights to privacy, a good name, and honor, which he considered had been violated as a result of an anonymous post on Blogger.com, owned by Google Inc., which claimed that the company Muebles Caquetá, owned by the plaintiff, was scamming its customers. Since this was the first time that Google Inc. itself had been sued, the response of the defendant was presented by the law firm Gómez-Pinzón Zuleta Abogados, as semi-official agent of Google Inc. The law firm stated that in its

> capacity as semi-official agent, under the terms of Article 57 of the CPC (sic), is necessary to the extent that (i) the corresponding – and required – power of attorney is in the process of being granted abroad, and (ii) in consideration of the domicile, Mountain View, California, United States, it is impossible for Google Inc. to respond to the aforementioned claim.[82]

Later, once the defendant company granted the corresponding power of attorney to the law firm, the latter stated that it was acting as the legal attorney of Google Inc. in Colombia, with special, broad, and sufficient power of attorney to represent it "in the aforementioned proceedings." Without any reservation about the semi-official agency, nor the subsequent legal representation of Google Inc. by the law firm Gómez-Pinzón Zuleta Abogados, the Constitutional Court ordered Google Inc., as owner of Blogger.com to delete the blog within the month following the judgment, as its content attributed, anonymously and without any evidence, the commission of the crime of "scamming" and other expressions that could be considered slander against the plaintiff and his company, and considering that the latter did not have any effective remedies

81 Ibid.

82 Constitutional Court, Judgment T-063A, 2017.

to obtain his claim. Likewise, the court warned that, so long as the subject of anonymous blogs with defamatory, disproportionate, libelous, or insulting content was not regulated in the content policy of Blogger.com, in cases where the party affected by this type of blog demonstrated that it did not have the ability to defend, contest, or rectify under equal conditions the information contained therein due to the anonymous nature of the publication, the content reported should be deleted without a court order.

Despite Google Colombia Ltda. reiterating its lack of passive legitimacy since "Google Colombia Ltda. and Google Inc. are two independent entities, each with a different domicile, legal person and corporate purposes," on this occasion the Constitutional Court provided the following, which we fully transcribe due to its importance:

> The first consideration is related to a precision that must be made between the two defending entities in this case: Google Inc. and Google Colombia Ltda. In fact, the aforementioned order will be mainly addressed against the company Google Inc. to the extent that, although Google Colombia Ltda. was also sued, during the review proceeding the latter mentioned that it does not represent the legal or corporate interests of Google in Colombia, but that it is only "a Google advertising management and sales agency, which has its independent legal personality and corporate purpose." However, several remarks must be made on the matter:
>
> (i) Although the Court understands that it refers to the exercise of different commercial and administrative duties under the same brand, this is not an obstacle for Google Colombia Ltda. to support management in compliance with the orders given to Google Inc., especially when the *latter is its parent company and has a shareholding interest in its Colombian affiliate*, as shown in the certificate of Incorporation and legal representation of Google Colombia Ltda., included in folio 45 of the file.
>
> (ii) Furthermore, *by performing activities in Colombia, both companies (Google Inc. and Google Colombia Ltda.) are obliged to respect the rights of the users and consumers of telecommunications and Internet services in the country*, as provided by the Constitution, the applicable law (Law 1341/2009 and Resolution 5111/2017 issued by the National Commission for Communications) and chapters 14 (Telecommunications) and 15 (E-commerce) of the Free Trade Agreement subscribed between Colombia and

the USA on the protection of the rights of the users and consumers of telecommunications and Internet services.

(iii) additionally, the *territorial presence of Google in Colombia not only implies an isolated commercial representation, it also implies legal and administrative responsibilities with the Colombian authorities regarding the protection of the rights of the users of telecommunications and Internet services which have been protected by the judgments issued by the competent national courts.* On this matter, it is worth reminding that, in several countries such as England (Tamiz *vs*. Google Inc. – 2014), Australia (Trkulja *vs*. Google Inc. – 2015), Canada (Pia Grillo *vs*. Google Inc. – 2014), Brazil (Daniela Cicarelli *vs*. Google Inc. – 2015) and the Hong Kong special administrative region (Yeung *vs*. Google Inc. – 2014 and Oriental Press Group *vs*. Fevaworks Solutions – 2013), among others, the company Google Inc. and its subsidiaries have faced similar disputes under which they have been ordered to comply with various court orders in cases of slander on websites, search engines and blogs that affect the rights of the users and consumers of telecommunications and Internet services.[83] (Italics added)

Based on these arguments, the Court ordered: (i) Google Colombia Ltda. to carry out all the actions required to make Google Inc. remove the content in dispute and send a report of such deletion to the Constitutional Court within the month following the service of this judgment; (ii) both companies, "in their capacity of *telecommunications and Internet services providers in Colombia*, to enroll on the ICT technology managed by the Ministry of Information and Communications Technologies, as provided by Law 1341/2009 (article 15) for companies whose activities and purpose correspond to the ICT sector with the purpose of offering greater assurances for the protection of the rights of the users and consumers of telecommunications and Internet services in the country."[84]

Based on this judgment, and as shown in Judgment T-121 of 2018 issued some time later, it seemed that the discussion about the passive legitimacy of Google Inc. on cases of alleged rights violations within the scope of the products the company offers in Colombia (the search engine

83 Ibid.
84 Ibid.

or YouTube platform, as in Judgment T-121 of 2018) had been solved. It seemed clear that whenever this type of company with no domicile in Colombia were to be held accountable before the competent Colombian authorities: (i) they would be *at least* responsible for the protection of the rights of the users and consumers of telecommunications and Internet services in the country (although the responsibility regarding the process of personal data by this type of company is still unaddressed); (ii) they would have to appoint an attorney-in-fact to represent them in the country; and (iii) their establishments in Colombia would also be accountable. However, through Writ 285 dated May 9, 2018, the Court ruled in favor of the appeal for annulment presented by Google Colombia Ltda., Google LLC (formerly Google Inc.),[85] and the MinTIC against the judgment. Thus, the court declared the nullity of the judgment for violation of due process, claiming that it omitted an analysis of three matters of constitutional relevance, whose review could have influenced the decision adopted and the orders given. The court considered that the judgment failed to address the prohibition of censorship contained in Article 20 of the Constitution, which makes paragraph 2 of the resolution section of the ruling enable some kind of censorship without prior legal order by imposing a constant monitoring obligation on Google for the automatic elimination of the content posted.

Second, it established that the difference between the person who creates the content and then publishes it, and the owner of the tool that only enables its publication was ignored, resulting in the determinations adopted regarding the publication being exclusively aimed at Google LLC, without presenting any appropriate justification to support them. According to the court, "the responsibility of the content creator for the statements classified as defamatory, disproportionate and slanderous in said ruling are not comparable to the rigor in the treatment provided to the Internet intermediaries who served as a means to host said degrading content."[86]

Finally, it considered that the relevant judgment failed to address that Google LLC is part of the category of content and applications providers (PCA, for its initials in Spanish), and not the category of

85 As mentioned, in September 2017 Google became a limited liability company (LLC) and stopped being a corporation.

86 Constitutional Court, Writ 285, 2018.

telecommunications networks and services providers (PRST, for its initials in Spanish). According to the court, exhausting this aspect would have led to a different decision, particularly regarding the regulatory provisions related to the enrollment on the ICT registry and the monitoring by the MinTIC of the activities performed by Google LLC.

Thus, although the causes for nullity mentioned by the court did not include the issue of the legal representation of Google LLC in Colombia, nor of the shared responsibility demanded of its Colombian affiliate, the fact is that Judgment T-063A of 2017 was annulled in its entirety. No legal precedent in Colombia currently specifies how CDDBMs not domiciled in Colombia may be held accountable.

4. CONCLUSIONS AND RECOMMENDATIONS

Following this analysis on how the CDDBMs included in our sample operate, on the gaps and flaws of the Colombian personal data protection regime, and on the capacity of the authorities to hold CDDBMs accountable, we have reached several conclusions. The business methods of the companies studied highlights the challenges that the digital age, the digital economy, and big data pose to the rights to the protection of data, to privacy, to equality, and to their related freedoms. Large volumes of digital data, along with current data analytics techniques, facilitate new sources of information (cookies in particular stand out as a technological tool for web tracking), with new data processing (without sufficient transparency on how algorithms and other technological tools used for descriptive, predictive, and prescriptive analysis function) and, mostly, with new purposes (data commercialization, personalized content, and automated decision-making being the most innovative) all with the possibility of profiling, whether as a tool or as an objective.

In turn, these new sources, processes, and purposes — particularly, the recurrent use of cookies, algorithms, and profiling — also show the deficiencies of our current data protection regime to deal with the risks of the digital age. These deficiencies relate both to the existence of inappropriate regulation and to the non-existence of any regulation at all or, in the best-case scenario, to the presence of provisions that may have the potential to meet the challenges of the digital age, but must be interpreted appropriately to do so.

Currently, the scope of our personal data protection law is insufficient for territorial application since it falls short regarding the processing of personal data carried out with "means" located outside of the country.

Likewise, this scope is not clear regarding controllers who, although not domiciled in the country, do have an establishment located in Colombia.

Lastly, the competent authorities have different levels of preparedness. On the one hand, a data protection authority with insufficient technical capability to address data exploitation and human rights matters. The provisions are currently blurry regarding the type of relationship to be maintained with the entities to be regulated, controlled, monitored, and sanctioned, with a focus on the "established" CDDBMs more than those arising in the digital age.[87] In terms of international cooperation, the law is quite timid when the rights of personal data subjects located outside of the Colombian territory are violated by the international collection of personal data. On the other hand, a constitutional court that, although empowered and intending to hold CDDBMs accountable, still cannot find the correct legal arguments[88] and continues without invoking the right to the protection of personal data to do so.

With such obvious room for improvement in ensuring the rights and freedoms of Colombians in the digital age, and in order to provide Colombia with a data protection framework that would provide the most up-to-date guarantees, we recommend the following:

1. Since our analysis was limited, it will be necessary to further develop the *academic research* on the scope and possible repercussions that the following elements might have on the rights and freedoms of Colombians:

---

87 On this matter, note that this characteristic is contradictory regarding the position expressed by the Superintendence of Industry and Commerce on the Guide for the Implementation of the Principle of Accountability. According to this guide: "Considering that the monitoring resources of the personal data protection policy are limited, its surveillance practice must focus towards the substandard entities with higher risks, on which the information processing causes a systemic risk with the potential of seriously affecting the data subjects" (italics added; SIC, n.d., p. 7). Not to say that the CDDBM included under the startups and "intermediate companies" categories are substandard; the fact is that the data exchange relationships which, as we saw, these companies usually have the GAFAM make on their behalf means that their processing of personal data could pose greater risks for the right to the protection of personal data than those posed by "established companies."

88 This because, as shown in Writ 285 of 2018, the protection of the rights of the users of the telecommunications networks and services providers does not seem to be the right way.

a. The power and control of GAFAM over the majority of the most popular applications and platforms in Colombia, and the internal and unrestricted exchange of data allowed between the products of the same corporate group.
b. The relationships between GAFAM and other CDDBMs pursuant to shared sign-ins and the insertion of Twitter, Google+, LinkedIn, or Facebook social buttons on the websites or apps of the CDDBMs.

2. To promote *greater doctrine and jurisprudential development* on the following:
   a. The concept of *personal data*, as set forth in Article 3(c) of Law 1581/2012, so that it is clear whether it includes other definitions of personal data, such as the IP address and similar identifiers, or the data related thereto.
   b. The concept of *sensitive data*, as set forth in Article 5 of Law 1581/2012, so that it is clear whether or not it includes not only the data that may affect the privacy of an individual or cause their discrimination, but also those which, although cause no risk in principle, allow inferring or deriving other sensitive data about its data subject when combined with other data.
   c. The possible nature of personal data control that content creators, Internet intermediaries, and those carrying out web crawling may have and their accountability regarding processing.
   d. The form in which CDDBMs not domiciled in Colombia may be held accountable.

   Such developments will clearly depend on larger participation by citizens or civil society through litigation, and on the submission of claims or requests for opinions before the Office of the Deputy Superintendence for the Protection of Personal Data. Although we are aware that the opinions issued by the Deputy Superintendence are not binding pursuant to Article 28 of Law 1437/2011, in fact, these will constitute a guide on the scope of said terms and questions both for judges and for entities obliged by law.
3. To obtain greater doctrinal, regulatory, legal, or jurisprudential developments on the following practices:
   a. Using cookies to collect personal data online, by imposing further limitations and safeguards to grant consent, except in the case of

cookies (i) essential for the operation of the service requested; or (ii) that collect anonymized data or data for aggregated use.

b. Profiling, which requires transparency and fairness in the profiling process, preventing opaque categorizations based on wrong or discriminatory data.

c. Processing data for *commercialization*, the *provision of personalized content* (particularly in the case of behavioral advertising), and *automated decision-making*, so that these are subject to greater safeguards than those offered by the principle of purpose under article 4(b) of Law 1571/2014.

d. *Sharing sensitive personal data for research purposes*, to provide greater restrictions on such exchanges, including anonymization and compliance with the four criteria of the compatibility assessment proposed by the Article 29 Working Party.

e. Obtaining *prior, express, and informed consent of the data subject* in profiling, making it mandatory to obtain consent for each specific purpose — data commercialization, behavioral advertising, or automated decision-making — expressed in a clear statement or affirmative action.

4. To *amend Law 1581/2012*, regarding the *scope of territorial application of the law*, so that it no longer depends on the location of the data controller or processor, its establishments, or the means it uses to process the data but rather depends on the location of the personal data subjects being processed.
5. To provide the Deputy Superintendence for the Protection of Personal Data with greater technical capabilities and human talent specialized in both data exploitation and human rights, to allow that office to face the technological and human rights challenges posed by the regulation of big data and the processing of personal data in the digital age.
6. To promote international cooperation with the data protection authorities of other countries when the rights of subjects located outside of Colombia are affected by the international collection of personal data.
7. That the CDDBMs complement their self-regulation measures by including the best practices identified in the privacy policies reviewed here in their own privacy policies, including the following:

a. That the content of messages sent by the user through the application or platform is not saved on the servers of the CDDBM, but rather on the user's device (a practice identified in the privacy policies of WhatsApp and 30 Day Fitness Challenge).
b. That user location data be collected anonymously (a practice adopted by Apple).
c. That, to the extent possible, the data collected through web tracking (log data and online data) are used only in aggregate or statistical form regarding how users, collectively, use the services (a practice identified on the privacy policy of Cívico).
d. That third parties be required to have legitimate rights to collect, use, or share any information received (a practice adopted by Facebook and Fluvip).
e. That third parties be required to respect the instructions of the CDDBM and comply with its conditions when using the information collected on their behalf (a practice identified on the WhatsApp and AliExpress privacy policies).
f. To specify the types of cookies used by the CDDBM to collect information (a practice identified on the Apple, 1DOC3, Biko, Tinder, and Netflix privacy policies).
g. That performance and functionality cookies only collect information anonymously (a practice adopted by Apple).
h. That, in the case of a reorganization, restructuring, merger, sale, or any other transfer of the CDDBM's assets, the transfer of information, including personal data, is subject to the receiver agreeing to respect the privacy policy of the entity who collected the data (a practice identified on the privacy policies of AliExpress and Netflix).
i. To make public the names of any third-party apps connected to the app of the CDDBM or used to sign-in, as well as the partners with whom the information is shared (a practice identified on the privacy policy of 8fit Workouts and Meal Planner).

Although these recommendations imply changes at several levels, it is essential to develop them as soon as possible to ensure that CDDBMs become accountable in Colombia before their growing economic, technological, and social power makes them impossible to control.

GLOSSARY

Algorithm: "Specific set of instructions, steps or processes to solve a specific problem. These allow clearly describing a series of instructions to be followed by a machine to achieve a predictable outcome" (TICbeat, 2017).

Application Programming Interface (API): "Set of subroutines, functions and procedures (or methods, in object-oriented programming) offered by a certain library to be used by another software as an abstraction layer" (TICbeat, 2017).

Biometric data: Data collected from "technologies that measure and analyze the characteristics of the human body, such as DNA, fingerprints, the retina and iris of the eyes, facial patterns or voice, and the measurements of the hands to authenticate the identity" (TICbeat, 2017).

Cookie: "A piece of information stored on your computer about Internet documents that you have looked at" (Cambridge Dictionary, n.d.).

Crowdsourcing: The collective construction of information through community participation in various tasks.

Data broker: "A person or company whose business is selling information about companies, markets, etc." (Cambridge Dictionary, n.d.).

Data mining: "The process of discovering processable information in large data sets. It uses mathematical analysis to deduce the patterns and trends in data" (TICbeat, 2017).

De-tag: "To [un]mark computer information [not] to be processed in a particular way" (Cambridge Dictionary, n.d.).

Geolocation: "Technology that shows the place where you are when using the Internet or a mobile phone" (Cambridge Dictionary, n.d.).

Global positioning system (GPS): "A system that can show the exact position of a person or thing by using signals from satellites" (Cambridge Dictionary, n.d.).

Internet Protocol Address (IP Address): "Number that identifies, in a logical and hierarchical form, the network interface (communication/connection element) of a device (computer, tablet, laptop, smartphone) that uses the IP (Internet Protocol) corresponding to the model TCP/IP at a network level" (TICbeat, 2017).

Machine learning: "Scientific discipline in the area of artificial intelligence which creates systems capable of automatic learning" (TICbeat, 2017).

Open data: "Philosophy and practice aimed at having certain type of data freely available to everybody, with no restrictions under copyright, patents, or other control mechanisms" (TICbeat, 2017).

Opt in: "To choose to be part of an activity, arrangement, etc." (Cambridge Dictionary, n.d.).

Opt out: "To choose not to be part of an activity or to stop being involved in it" (Cambridge Dictionary, n.d.).

Profiling: "The practice or method of preparing a set of characteristics belonging to a certain class or group of people or things by which to identify individuals as belonging to such a class or group" (Collins Dictionary, n.d.).

Uniform Resource Locator (URL): "The Internet address for a website" (Cambridge Dictionary, n.d.).

Web crawling: The use of computer software to browse the web and index its contents; for example, web crawling is used by the Google Search platform to show search results.

Web tracking: Tracking mechanisms that identify the tools we use on the Internet, such as the device, Wi-Fi network, and browser, among others.

REFERENCES

Alcaíno, M., Arenas, V., & Gutiérrez, F. (2015). *Modelos de negocios basados en datos: desafíos del big data en Latinoamérica*. Santiago, Chile: Universidad de Chile.

App Annie. (2018). Top App Matrix. Retrieved from https://www.appannie.com/dashboard/home/

BNamericas. (2017, July 20). Ranking de aseguradoras colombianas. Retrieved from http://www.bnamericas.com/es/noticias/seguros/ranking-de-aseguradoras-colombianas/

Cambridge Dictionary. (n.d.). Available at https://dictionary.cambridge.org/es/

Collins Dictionary. (n.d.). Available at https://www.collinsdictionary.com/es/

Colombia Digital. (2013). Infografía: "¿Cómo están posicionados los gigantes de Internet?" Retrieved from https://colombiadigital.net/images/infografias/como-estan-posicionados-los-gigantes-de-internet.jpg

Corredor, G. R. (2015). Consolidación de la economía digital y desafíos en materia de protección de la privacidad. *Revista de derecho, comunicaciones y tecnologías, 14*, 1–26.

Constitutional Court, Judgment T-222, 1992, Speaker Judge Ciro Angarita Barón.

Constitutional Court, Judgment T-406, 1992, Speaker Judge Ciro Angarita Barón.

Constitutional Court, Judgment T-414, 1992, Speaker Judge Ciro Angarita Barón.

Constitutional Court, Judgment T-729, 2002, Speaker Judge Eduardo Montealegre Lynett.

Constitutional Court, Judgment C-150, 2003, Speaker Judge Manuel José Cepeda Espinosa.

Constitutional Court, Judgment C-748, 2011, Speaker Judge Jorge Ignacio Pretelt Chaljub.

Constitutional Court, Judgment T-040, 2013, Speaker Judge Jorge Ignacio Pretelt Chaljub.

Constitutional Court, Judgment T-277, 2015, Speaker Judge María Victoria Calle Correa.

Constitutional Court, Judgment C-542, 2015, Speaker Judge Humberto Antonio Sierra Porto.

Constitutional Court, Judgment T-063A, 2017, Speaker Judge Jorge Iván Palacio.

Constitutional Court, Judgment T-121, 2018, Speaker Judge Carlos Bernal Pulido.

Constitutional Court, Writ 285, 2018, Speaker Judge José Fernando Reyes Cuartas.

Court of Justice. (2014). Google Spain, S.L., and Google Inc. *vs*. Spanish Data Protection Agency and Costeja González, May 13, 2014. Court of Justice of the European Union.

Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated experiments on ad privacy settings. *Proceedings on Privacy Enhancing Technologies, 1*, 92–112.

De Mauro, A., Greco, M., & Grimaldi, M. (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, Madrid, Spain, September 5–8, 2014.

El Tiempo. (2017, June 14). Estas son las compañías más grandes que operan en Colombia. Retrieved from https://www.eltiempo.com/economia/empresas/10-empresas-mas-grandes-de-colombia-98992

Dorantes, R. (2018). Qué es una startup. *Entrepreneur*, 22 August 2018. Retrieved from https://www.entrepreneur.com/article/304376

European Commission (EC). (1998). Judging industry self-regulation: When does it make a meaningful contribution to the level of data protection in a third country? Working document DG XV D/5057/97. Adopted on 14 January 1998. Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp7_en.pdf

European Commission (EC). (2000). Working document: Privacy on the Internet — An integrated EU approach to on-line data protection. November 21, 2000. Article 29 Working Party, 5063/00/EN/FINAL WP 37. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf

European Commission (EC). (2010). Opinion 2/2010 on online behavioral advertising, adopted June 22, 2010. Article 29 Working Party, 00909/10/EN WP 171. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

European Commission (EC). (2012). Opinion 4/2012 on cookie consent exemption, adopted June 7, 2012. Article 29 Working Party, 00879/12/EN WP 194. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

European Commission (EC). (2013). Opinion 03/2013 on purpose limitation, adopted April 2, 2013. Article 29 Working Party, 00569/13/EN WP 203. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

European Commission (EC). (2017a). Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679, adopted October 3, 2017. Article 29 Working Party, 17/EN WP251 rev. 01. Retrieved from https://ec.europa.eu/newsroom/document.cfm?doc_id=47742

European Commission (EC). (2017b). Proposal for an ePrivacy regulation. Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

European Commission (EC). (2018). Working document: Guidelines on consent under Regulation 2016/679, adopted April 10, 2018. Article 29 Working Party, 17/EN WP259 rev.01. Retrieved from https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030

Federal Trade Commission (FTC). (2016). FTC issues warning letters to app developers using "Silverpush" code. Retrieved from https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpushcode

Federal Trade Commission (FTC). (2017). Cross-device tracking: An FTC staff report. Retrieved from https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race and the future of law enforcement.* New York: New York University Press.

Forbrukerradet. (2018, June 6). Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy. Retrieved from https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Hartmann, P. M., Zaki, M., Feldmann, N., & Hartmann, A. N. (2014). *Big data* for big business? Blog. Cambridge: Cambridge Service Alliance.

Haupt, M. (2016). "Data is the new oil": A ludicrous proposition. Retrieved from https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294

Hern, A., & Pegg, D. (2018). Facebook fined for data breaches in Cambridge Analytica scandal. *The Guardian*, 11 July 2018. Retrieved from: https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal

Hill, K. (2012). How Target figured out a teen girl was pregnant before her father did. *Forbes*, 16 February 2012. Retrieved from https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4f3623b66668

Ibero-American Data Protection Network (IADPN). (2006). Autorregulación y protección de datos personales. Document prepared by the Working Party meeting in Santa Cruz de la Sierra, Bolivia, May 3–5.

INNpulsa Colombia. (n.d.). Las mejores *start-ups* colombianas para invertir. Retrieved from https://www.innpulsacolombia.com/sites/default/files/civico_0.pdf

Kay, M., Matuszek, C., & Munson, S. A. (2015). Unequal representation and gender stereotypes in image search results for occupations. Paper presented at the Conference on Human Factors in Computing Systems (CHI), Seoul, Republic of Korea, April 18–23.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). *Big data: The next frontier for innovation, competition, and productivity.* New York: McKinsey Global Institute.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work and think*. New York: Mariner Books.

McDonald, A. M. (2018). Statement of Aleecia M. McDonald, PhD, Assistant Professor of the Practice, Information Networking Institute, Carnegie Mellon University, Member of the Board of Directors, Privacy Rights Clearinghouse. California Assembly Committee on Privacy and Consumer Protection. The California Consumer Privacy Act of 2018. Retrieved from http://www.archive.ece.cmu.

edu/~ece734/readings/CA-Assembly-June26-2018-McDonald-testimony.pdf

McGuire, A. (2018). Interview with the European data protection supervisor Giovanni Buttarelli: The GDPR is a radical update of the rule book for the digital age. *Irish Tech News*, 24 July 2018. Retrieved from https://irishtechnews.ie/interview-with-the-european-data-protection-supervisor-giovanni-buttarelli-the-gdpr-is-a-radical-update-of-the-rule-book-for-the-digital-age/

McNeil, J. (n.d.). Big brother's blind spot: Mining the failures of surveillance tech. *The Baffler*. Retrieved from https://thebaffler.com/salvos/big-brothers-blind-spot-mcneil

Nonsoque, J. C. (2018). Ingresos del top 10 de las compañías de telecomunicaciones sumaron $28 billones. *La República*, 21 May 2018. Retrieved from https://www.larepublica.co/especiales/las-empresas-mas-grandes-de-2017/ingresos-del-top-10-de-las-companias-de-telecomunicaciones-sumaron-28-billones-2728972

Noyb. (2018, May 25). GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook. Retrieved from https://noyb.eu/4complaints/

Organization of American States (OAS). (2015). Report by the Inter-American Juridical Committee: Privacy and protection of personal data. 86th Ordinary Period of Sessions. CJI/doc. 474/15 rev.2 adopted March 26, 2015.

Portafolio. (2017, October 1). Éxito y Zara, los líderes en "retail." Retrieved from http://www.portafolio.co/negocios/empresas/empresa-lideres-en-retail-en-colombia-510250

Restrepo, M. A. (2009). Derecho administrativo contemporáneo: ¿derecho administrativo neopolicial? En *Retos y perspectivas de derecho administrativo. Segunda parte*. Bogotá: Editorial Universidad del Rosario.

Schneir, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world.* New York: Norton & Company.

Search Data Center. (n.d.). Definition Política de Privacidad. Retrieved from https://searchdatacenter.techtarget.com/es/definicion/Politica-de-privacidad

Serrato, J. K., Cwalina, C., Rudawski, A., Coughlin, T., & Fardelmann, K. (2018). US states pass data protection laws on the heels of the GDPR. *Data Protection Report.* Retrieved from https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/

Statista. (2018a). Number of Internet users in Latin America from 2014 to 2019 (in millions). Retrieved from https://www.statista.com/statistics/274860/number-of-internet-users-in-latin-america/

Statista. (2018b). Share of desktop search traffic originating from Google in Latin America in August 2017, by country. Retrieved from https://www.statista.com/statistics/639072/googles-share-of-search-market-in-selected-countries-latam/

Statista. (2018c). Number of Facebook users in Latin America from 2014 to 2019 (in millions). Retrieved from https://www.statista.com/statistics/282350/number-of-facebook-users-in-latin-america/

Statista. (2018d). Number of digital buyers in Latin America from 2014 to 2019 (in millions). Retrieved from https://www.statista.com/statistics/251657/number-of-digital-buyers-in-latin-america/

Superintendence of Industry and Commerce (SIC). (n.d.). Guía para la implementación del principio de responsabilidad demostrada (Accountability). Ministry of Commerce, Industry and Tourism, Colombia. Retrieved from http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

Superintendence of Industry and Commerce (SIC). (2014a). Resolution 36863 dated May 30, 2014. Ministry of Commerce, Industry and Tourism, Colombia. Retrieved from http://www.sic.gov.co/sites/default/files/files/Res%20No_%2036863%20de%202014%20-%20ALMACENES%20EXITO.pdf

Superintendence of Industry and Commerce (SIC). (2014b). Opinion 14-218349-00003-0000 dated November 24, 2014. Ministry of Commerce, Industry and Tourism, Colombia.

Superintendence of Industry and Commerce (SIC). (2016a). Opinion 14-218349-4-0, dated March 3, 2016. Ministry of Commerce, Industry and Tourism, Colombia.

Superintendence of Industry and Commerce (SIC). (2016b). Opinion 16-172268-00001-0000 dated August 9, 2016. Ministry of Commerce, Industry and Tourism, Colombia.

Superintendence of Industry and Commerce (SIC). (2016c). Resolution 85568 dated December 13, 2016. Ministry of Commerce, Industry and Tourism, Colombia. Retrieved from http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE85568-2016.pdf

Superintendence of Industry and Commerce (SIC). (2017). Resolution 78911 dated November 30, 2017. Ministry of Commerce, Industry and Tourism, Colombia. Retrieved from http://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/Resolucion_78911_2017.pdf

Superintendence of Industry and Commerce (SIC). (2018a). Resolution 44026 dated June 25, 2018. Ministry of Commerce, Industry and Tourism, Colombia. Retrieved from http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE44026-2018.pdf

Superintendence of Industry and Commerce (SIC). (2018b). Sanctions to personal data protection. Ministry of Commerce, Industry and Tourism, Colombia. Retrieved from http://www.sic.gov.co/sanciones-2018

Team Startup Colombia. (2017). ¿Qué es? Retrieved from http://micrositios.mintic.gov.co/team-startup/

Terms Feed. (2018). Privacy policies *vs.* terms and conditions. Retrieved from https://termsfeed.com/blog/privacy-policies-vs-terms-conditions/#A_single_agreement_or_separate

TICbeat. (2017). Diccionario para saber todo sobre datos en la era digital. Retrieved from http://www.ticbeat.com/tecnologias/diccionario-para-saber-todo-sobre-datos-en-la-era-digital/

World Economic Forum (WEF). (2011). Personal data: The emergence of a new asset class. Retrieved from http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

Annex 1. Privacy Policies Consulted

1DOC3 S.A.S. Manual of policies and procedures to protect and process personal data. Last update: March 1, 2014. Retrieved from https://www.1doc3.com/web/politicas

Alibaba Group. Privacy Policy. Last update: May 24, 2018. Retrieved from http://rule.alibaba.com/rule/detail/2034.htm

Almacenes Éxito S.A. Information and personal data management policy. Last update: February of 2014. Retrieved from https://www.grupoexito.com.co/files/Poltica_manejo_de_informacin_y_datos_personales_3.pdf

Amazon Inc. Privacy notice. Last update: August 29, 2017. Retrieved from https://www.amazon.com/gp/help/customer/display.html?language=es_US&nodeId=468496

Apple Inc. Privacy policy. Last update: May 22, 2018. Retrieved from https://www.apple.com/legal/privacy/en-ww/

Acsendo S.A.S. Personal data protection policy. Last update: June 30, 2017. Retrieved from https://www.acsendo.com/es/privacidad/

Bending Spoons S.p.A. Privacy policy. No date for last update. Retrieved from https://bendingspoons.com/privacy.html

Biko Development Inc. Privacy policy. No date for last update. Retrieved from https://bikoapp.com/policy.html

Cívico Digital S.A.S. Personal data processing policy. Last update: December 7, 2017. Retrieved from https://www.civico.com/politicas-de-privacidad

Deezer SA. Privacy and cookies policy. No date for last update. Retrieved from https://www.deezer.com/legal/personal-datas

Duety S.A.S. Legal. Last update: February 14, 2018. Retrieved from https://blog.duety.co/legal/#privacidad

Easy Taxi Colombia S.A.S. Privacy notice. No date for last update. Retrieved from http://www.easytaxi.com/co/terms-conditions/aviso-de-privacidad/

Facebook Inc. Data policy. Last update: April 19, 2018. Retrieved from https://www.facebook.com/privacy/explanation

Facebook Inc. WhatsApp privacy policy. Last update: April 24, 2018. Retrieved from https://www.whatsapp.com/legal?eea=0#privacy-policy

FLUVIP S.A.S. FLUVIP policy for the protection and processing of personal data. No date for last update. Retrieved from http://www.fluvip.com/home_policy_for_the_protection?locale=es_CO

Google LLC. Google privacy policy. Last update: May 25, 2018. Retrieved from https://policies.google.com/privacy?hl=es-US&gl=us

Grupo Aval Acciones y Valores S.A. Privacy and personal data processing policy. No date for last update. Retrieved from https://www.grupoaval.com/wps/wcm/connect/grupo-aval/2c470a75-992f-4db3-a47b-a70da487464b/Politica-Tratamiento-Datos-Personales.pdf?MOD=AJPERES

Inversiones CMR S.A.A. Privacy and personal data processing policy. Last update: February 27, 2018. Retrieved from https://domicilios.com/pages/politica-de-privacidad.html

IoT Services Inc. Privacy policy. No information on last update. Retrieved from https://ubidots.com/privacy-policy/

Match Group, LLC. Our commitment to you. Last update: May 25, 2018. Retrieved from https://www.gotinder.com/privacy?locale=es

Microsoft Corporation. Microsoft privacy statement. Last update: August of 2018. Retrieved from https://privacy.microsoft.com/es-mx/privacystatement#mainhowtoaccesscontrolyourdatamodule

Microsoft Corporation. LinkedIn privacy policy. Last update: May 8, 2018. Retrieved from https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv

Netflix International B.V. Privacy statement. Last update: May 11, 2018. Retrieved from https://help.netflix.com/legal/privacy

Rappi S.A.S. Privacy notice. No information on last update. Retrieved from http://wordpress.rappi.com.br/terms-conditions/

Seguros Generales Suramericana S.A. Privacy and personal data processing policy. Last update: June 16, 2017. Retrieved from https://www.segurossura.com.co/Paginas/legal/politica-privacidad-datos.aspx

SIA Joom (Latvia). Joom privacy policy. No information on last update. Retrieved from https://www.joom.com/es/privacy

Spotify AB. Spotify privacy policy. Last update: May 25, 2018. Retrieved from https://www.spotify.com/co/legal/privacy-policy/

Telmex Colombia S.A. Information processing policy. Last update: July 26, 2013. Retrieved from https://www.claro.com.co/portal/recursos/co/legal-regulatorio/pdf/Politicas_Seguridad_Inf_Claro.pdf

Uber B.V. Privacy policy. Last update: May 25, 2018. Retrieved from https://privacy.uber.com/policy

Urbanite Inc. Privacy policy. No information on last update. Retrieved from https://8fit.com/privacy/

Unilever N.V. Privacy notice. No information on last update. Retrieved from https://www.unileverprivacypolicy.com/spanish/policy.aspx

Waze Mobile Limited. Privacy policy. Last update: May 25, 2018. Retrieved from https://www.waze.com/es-419/legal/privacy

Annex 2. Types of Data-Driven Business Models

Data sources	*Internal sources*	Data currently existing in the CDDBMs	
		Data generated via monitoring	Web tracking
			Sensors
			Crowdsourcing
	External sources	Data provided by the client	
		Data provided by strategic partners	
		Data acquired	
		Data freely available on the Internet	Open data
			Social Media Sites
			Web crawling
Key activities	*Aggregation*		
	Analysis	Descriptive	
		Predictive	
		Prescriptive	
	Distribution		
	Visualization		
Client segment	*Business to Consumer (B2C)*		
	Business to Business (B2B)		
	Business to Consumer to Business (B2C2B)		
Value proposition	*Data*		
	Information and knowledge		
	Non-digitized goods and services		
	Improved goods and services		
	Digitized physical assets		
	Data combinations		
	Data commercialization		
	Process coding		
Revenue creation model	*Advertisement*		
	Sale		
	Leasing/Loan		
	Licensing		
	Freemium		
	Charge for use		
	Price per project		
	Subscription		
	Commission		
Data structure	*Effort to create data*		
	Data created as a by-product of its activities		

SOURCE: Based on Hartmann et al. (2014) and Alcaíno et al. (2015).

Annex 3. Focus Group Attendees

On November 20, 2018, a focus group met at the Dejusticia offices to discuss the document "Accountability of Google and Other Businesses in Colombia: Personal Data Protection in the Digital Age."

	Entity	Representative
1	Fundación Karisma	Juan Diego Castañeda
2	Linterna Verde	Carlos Cortés
3	Consejo Privado de Competitividad	Lorena Lizarazo
4	Universidad Externado	Camilo de la Cruz
5		Daniel Castaño
6	Universidad del Rosario	Grenfieth Sierra
7	Former Deputy Superintendent for the Protection of Personal Data (2012–2015)	José Alejandro Bermúdez
8	Supreme Court of Justice	Ana Carolina Molina
9	UNICEF Big Data consultant	Viviana Cañón
10	Privacy International	Aillidh Callander (vía Bluejeans)
11	Omidyar	Gabriela Hadid (vía Bluejeans)
12	Dejusticia	Vivian Newman
13		María Paula Ángel
14		Laura Guerrero
15		Celso Bessa
16		Sophie Kushen

Representatives of the following state entities, academia, civil society, and companies were also invited, but did not attend the focus group:

- Deputy Superintendence for the Protection of Personal Data
- Directorate for the Development of the IT industry of the Ministry of Information and Communications Technologies (MinTIC)
- Office of the Magistrate Fernando Reyes Cuartas (speaker judge of Writ 285/18)
- Internet and Society Center of Universidad del Rosario
- Group for Internet, E-trade, Telecommunications and Informatics Studies (GECTI, for its acronym in Spanish) of Universidad de los Andes
- Center for Research on IT Law and New Technologies of Universidad Externado de Colombia
- Office of the Dean of the School of Law of Universidad de los Andes

- Fundación para la Libertad de Prensa (FLIP)
- ENter.co
- Accessnow
- Media Legal Defence Initiative
- Tech & Law
- Data&Tic
- Microsoft Colombia
- Facebook
- Samsung
- Rappi
- Google Colombia

In the case of Google Colombia, we were able to hold a video conference, wherein they expressed their interest in sending their comments on the document. However, to date we have not received any communication on the matter.

Annex 4. App Store Most Downloaded Applications (First five days of July, August, and September of 2018)

iPhone Top App Matrix										
7/1/2018	DirectTV Sports	DirectTV	WhatsApp	Instagram	YouTube	Netflix	Deezer	Tinder	LinkedIn	8fit
7/2/2018	DirectTV Sports	DirectTV	WhatsApp	30 Days Fitness Challenge	Instagram	Netflix	Deezer	Tinder	Clash Royale	Candy Crush Saga
7/3/2018	DirectTV Sports	DirectTV	WhatsApp	Messenger	Selección Colombia Oficial	Netflix	Deezer	Tinder	Dropbox	Clash Royale
7/4/2018	WhatsApp	Messenger	Instagram	Facebook	YouTube	Netflix	MARVEL Contest of Champions	Deezer	Tinder	LinkedIn
7/5/2018	WhatsApp	Instagram	Facebook	Messenger	YouTube	Netflix	Tinder	Deezer	Sniper 3D	MARVEL Contest of Champions
8/1/2018	WhatsApp	Facebook	Messenger	Instagram	YouTube	Netflix	Deezer	Tinder	Candy Crush Saga	Captain Tsubasa
8/2/2018	WhatsApp	Messenger	Facebook	Instagram	YouTube	Netflix	Deezer	LinkedIn	Tinder	App removed
8/3/2018	WhatsApp	Messenger	Facebook	Instagram	YouTube	Netflix	Deezer	Tinder	App removed	LinkedIn
8/4/2018	WhatsApp	Facebook	Instagram	Messenger	YouTube	Netflix	Deezer	Tinder	LinkedIn	App removed
8/5/2018	WhatsApp	YouTube	Facebook	Instagram	Messenger	Netflix	Tinder	Deezer	LinkedIn	Fortnite
9/1/2018	Hello Star	WhatsApp	YouTube	AliExpress	Messenger	Netflix	Tinder	Deezer	Luxy Millionaire	Candy Crush Saga
9/2/2018	Hello Star	YouTube	WhatsApp	Facebook	Instagram	Netflix	Deezer	Tinder	LinkedIn	Summoners War
9/3/2018	WhatsApp	Hello Star	Facebook	Messenger	YouTube	Netflix	Tinder	Deezer	Clash Royale	LinkedIn
9/4/2018	WhatsApp	Facebook	Messenger	Instagram	YouTube	Netflix	Deezer	Tinder	LinkedIn	Clash Royale
9/5/2018	WhatsApp	Facebook	Messenger	Instagram	YouTube	Netflix	Clash Royale	Deezer	Tinder	LinkedIn

Annex 5. Google Play Most Downloaded Applications (First five days of July, August, and September of 2018)

Google Play Top App Matrix										
7/1/2018	WhatsApp	Messenger	Facebook Lite	Facebook	Instagram	Google Drive	Tinder	Lords Mobile	King of Avalon	Clash Royale
7/2/2018	WhatsApp	Messenger	App removed	Facebook Lite	Facebook	Google Drive	Tinder	Lords Mobile	Clash Royale	Captain Tsubasa
7/3/2018	WhatsApp	Messenger	App removed	Facebook Lite	Facebook	Google Drive	Tinder	Clash Royale	Lords Mobile	Captain Tsubasa
7/4/2018	WhatsApp	Messenger	Facebook Lite	Rise Up	Instagram	Google Drive	Tinder	Clash Royale	Lords Mobile	Captain Tsubasa
7/5/2018	WhatsApp	Messenger	Facebook Lite	Rise Up	Instagram	Google Drive	Tinder	Clash Royale	Lords Mobile	Captain Tsubasa
8/1/2018	WhatsApp	Messenger	Facebook Lite	Facebook	Instagram	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
8/2/2018	WhatsApp	Messenger	Facebook Lite	Facebook	Joom	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
8/3/2018	WhatsApp	Messenger	Facebook Lite	Facebook	Messenger Lite	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
8/4/2018	WhatsApp	Messenger	Facebook Lite	Facebook	Messenger Lite	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
8/5/2018	WhatsApp	Messenger	Facebook Lite	Facebook	Instagram	Google Drive	Tinder	Lords Mobile	Garena Free Fire	Clash Royale
9/1/2018	Hello Star	AliExpress	WhatsApp	Facebook Lite	Messenger	Google Drive	Tinder	Lords Mobile	Garena Free Fire	Clash Royale
9/2/2018	WhatsApp	Messenger	Facebook Lite	Hello Star	Facebook	Google Drive	Tinder	Lords Mobile	Garena Free Fire	Clash Royale
9/3/2018	WhatsApp	Messenger	Hello Star	Facebook Lite	Facebook	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
9/4/2018	WhatsApp	Messenger	Hello Star	Facebook Lite	Facebook	Google Drive	Garena Free Fire	Tinder	Clash Royale	Lords Mobile
9/5/2018	WhatsApp	Messenger	Facebook Lite	Hello Star	Facebook	Google Drive	Garena Free Fire	Clash Royale	Tinder	Lords Mobile

DEJUSTICIA WORKING PAPER SERIES

• 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

PALIATIVE 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

WORKING PAPER 7

In 2018 The European Union General Data Protection Regulation became effective and the California Consume Privacy Act was enacted. Both regulations are aimed at balancing the development of the digital economy with the protection of the rights to privacy and the protection of personal data. How? By regulating the new data sources, types and purposes of processing in the digital age and which include the use of cookies, web crawling, algorithms, profiling, automated decision-making, data commercialization and behavioral advertising. What has been done in Colombia to ensure these rights in the framework of the digital economy? In this document we explore how prepared are our competent authorities and our personal data protection legal regime to face the challenges that the digital age poses for different values and rights, thus holding the companies with data-driven business models (CDDBMs) accountable. For this, based on a review of their privacy policies, we analyze the operations of an illustrative sample of 30 CDDBMs, within which GAFAM (Google, Apple, Facebook, Amazon, and Microsoft) stand out, due to their economic, technological and social power.

978-958-5597-00-6

9 789585 597006