UiO : Faculty of Law
University of Oslo

Challenges of Colombian Data Protection Framework

Towards a European Adequate Level of Protection

Candidate number: 7006

Submission deadline: 01/12/2018

Number of words: 17500

TABLE OF CONTENTS

1. INTRODUCTION

It is undeniable that with the rapid development of technology in recent years, large companies such as Google, Facebook, and Amazon, among others, are a reference in today's economy.[1] In fact, six out of ten of the top richest men in the world are founders of tech companies and a large portion of their fortune is mainly due to the processing of data through artificial intelligence mechanisms to increase the success of marketing and advertising. Personal data is of such importance that even the president of the European airline SAS stated that the information registered in their databases represented a greater economic value than the entire fleet of the company.[2] Therefore, the data of people is considered by many as the "new oil" of the 21st century, which makes it a precious commodity for large tech companies.[3]

However, unlike oil, personal data regulated by data protection law is considered a fundamental right in many constitutions and international treaties around the globe, which is why it is a very important topic for legal systems. It is perhaps the first time in the history of humankind that a fundamental right has so much economic interest, which presupposes great challenges for legislators when discussing this type of law. For the European Union, privacy is not a commodity to be traded, as was stated in 2015.[4]

Aware of such importance, some countries and international organizations have developed legal frameworks which, according to the core principles and efficient mechanisms

[1] https://www.usatoday.com/story/money/2018/03/06/jeff-bezos-unseats-bill-gates-forbes-2018-richest-billionaires-list/398877002/ Last Accessed March 2018
[2] Comments of Professor Bygrave, L. UIO Data Protection Lecture
[3] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data Last Accessed December 2017
[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Trade for All Towards a more responsible trade and investment policy, COM(2015) 497 final, 14.10.2015, p. 7.

established in their privacy legislations, aim to guarantee similar levels of data protection of the personal data that flows between countries.[5]

One of the most progressive examples in this field is the work done by the European Union (hereinafter, "EU"). The EU first became an international reference in this field with Convention 108 of 1981 of the European Council and later when issuing the Data Protection Directive (hereinafter, "DPD") of 1995. According to Articles 25 and 26 of the DPD, which developed the legal concept of adequate levels of protection, a transfer of personal data to countries outside the EU / EEA can only take place in the event that those countries guarantee minimum data protection standards.

Since the DPD was issued, just few countries from different latitudes and legal systems have been recognized as providing adequate levels of protection.[6] From those countries, only two Latin American countries, Argentina in 2003 and Uruguay in 2012, have achieved that recognition by the European Commission. Latin American countries, as a general rule, have similar legal systems that have been greatly influenced by the European Roman Civil Law.[7] For this reason, new regulations developed in the region are frequently analyzed to determine their relevance and eventual adoption. This influence was also reflected in the foundation of the Ibero-American Network for the Protection of Personal Data in Guatemala (2003), with the active participation of European entities such as the Spanish Data Protection Agency, current member of the organization, and the EU as an observer.[8]

The Republic of Colombia has also been guided by that framework. Although it took around 20 years to issue a comprehensive set of rules after establishing the right to privacy as fundamental in its Political Constitution of 1991, the decisions of the Constitutional Court

[5] For instance, European Union Data Protection Framework has inspired many regulations worldwide.
[6] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en Last Accessed May 2017
[7] https://www.law.berkeley.edu/library/robbins/CommonLawCivilLawTraditions.html Last Accessed June 2017
[8] Nelson Remolina-Angarita, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010).

on this matter have been endowed with clear European influence of the DPD. Moreover, with the adoption of a free trade agreement with the EU, Colombia saw the need to achieve a recognition of an adequate level of protection by the European Commission in order to generate a competitive legal framework that facilitates the conduction of business.[9]

In order to achieve this goal, the Colombian Congress issued a General Data Protection Act in 2012 that is inspired by the principles of the DPD. However, recently the EU has replaced the DPD by the new General Data Protection Regulation[10] (hereinafter, the GDPR), which implies new challenges for Colombia to obtain European recognition as a third country with an adequate level of protection.[11]

1.1 Questions and Problems Considered

The main question addressed in this paper addresses whether the current Colombian data protection framework has an adequate level of protection according to the European standard. The question is particularly relevant since the European Parliament has recently replaced the DPD, introducing new changes to its data protection regime while at the same time the Colombian government seeks to be recognized by the EU as a third country with an adequate level of protection. In fact on February 14, 2013, the Colombian Ministry of Foreign Affairs formally submitted a request to the EU to start the process of recognition according to Article 25 of the DPD.[12]

Until now the EU has only recognized a few countries as having an adequate level of protection, but because that recognition was made according to the DPD, important questions

[9] Ibid
[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)
[11] Ibid
[12] December 7th 2017 Reply letter from the Director of the Colombian Data Protection Authority, Dra. María Claudia Caviedes Mejía.

arise when studying the new methodology the EU will adopt in order to analyze the level of protection of a new country regarding the GDPR. As the GDPR became effective on May 25, 2018, there is no definitive document on a final adequacy decision to date. Only in September 2018 did the Commission release a draft on Japan, in which it can be seen that it carries out an exhaustive study of the entire Japanese legal system in relation to data protection. The draft contains approximately 30,000 words, so this thesis with a word limit requirement seek to highlight some important aspects of the Colombian data protection framework that the European Commission (hereinafter, "EC") should take into account when analyzing the Colombian legal system under the GDPR. To carry out such work, previous assessments made by the Article 29 Working Party will be vital to determine the fundamental aspects that the EC takes into account when doing this type of assessment, as well as predicting novelties under GDPR. Also vital will be guidance from the draft released about Japan, but it should be noted that the draft was released when the development this thesis was already well advanced.[13] [14]

Therefore, the first chapter will present the European Commission's considerations when assessing an adequate level of protection analysis. The second chapter will be focused on current Colombian data protection framework, analyzing Article 15 of 1991 Colombia Constitution and relevant case law made by Colombian Constitutional Court. The third chapter will address Colombian Regulation analyzing GDPR's particularities and the last Chapter will analyze the new criteria set out by the European Commission and how it will be evaluated regarding the Colombian legal system. This work plan will allow us to identify the challenges Colombian data protection framework is facing an order to achieve an adequate level of protection European standard.

[13] http://europa.eu/rapid/press-release_IP-18-5433_en.htm Last Accessed September 2018
[14] https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf Last Accessed September 2018

2. EUROPEAN ADEQUATE LEVEL OF PROTECTION

2.1 Data Protection Directive

Although the DPD is no longer binding as it has been replaced by the GDPR, its analysis is of vital importance since it was a pioneer in establishing the parameters to grant an adequate level of protection to third countries. Therefore, both the directive and the new GDPR will be analyzed in order to understand the key elements the EC will revise when assessing an adequate level study on third countries data protection framework.

Article 25 of the DPD established that a transfer to a third country of personal data can only be carried out when the third country concerned guarantees an adequate level of protection. Hence, it is necessary to establish what is meant by "adequate level." According to the Collins dictionary, the word adequate means: "able to fulfil a need or requirement without being abundant, outstanding, etc."[15] Notice that the definition never uses the words equal or same, thus, in order to be considered adequate, it does not imply that the legal framework of the third country should be identical, but that the legal system must meet certain requirements or standards. This was confirmed by Article 29 Working Party in 1998 which pointed out that adequacy does not necessarily imply equivalency with EU standards.

However, the Schrems landmark decision the European Court of Justice raised the bar by stating that: "the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter (…)"[16]

[15] English Collins Dictionary. Available at: http://dictionary.reverso.net/english-definition/adequate%20level

[16] Court of Justice of the European Union, C-362/14, 6 October 2015. http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=8101969 Last Accessed March 2018.

It is important to emphasize that this same parameter applies today to the GDPR. Article 25 (2) of the DPD laid out some criteria for the assessment of adequacy, stating that it: "shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."[17]

Although the directive tried to provide guidelines for interpretation, the language was too broad and vague. For this reason, the Article 29 Working Party developed this concept better and provided a series of documents as a reference.

2.2 Article 29 Working Party

According to Article 29 of the DPD, a Working Party on the protection of individuals with regard to the processing of Personal Data shall have advisory status and will act independently. The Article 29 Working Party issued two documents that set up possible ways to evaluate the level of protection of third countries. In these documents, The Article 29 Working Party made it clear that a level of adequate protection depends on several factors, some regulatory and others "instrumental and institutional."[18]

The first of these factors is the result of a mixture of rights of the data subject and obligations for those who process the personal information or exercise control over that treatment. The second refers to the existence of mechanisms, both judicial and non-judicial procedures, which guarantee the effectiveness of the rules; such as sanctions when non-compliance or

[17] Article 25 EU DIRECTIVE 95/46/EC
[18] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf Last accessed July 2017

data breaches occur and the redress mechanisms that the data subject can exercise to demand respect for their rights. Additionally, it considers the existence of an independent authority that not only controls, monitors, and sanctions those who do not comply with the regulation, but also to receive complaints from data subjects and to start relevant investigations.

Therefore, it was specified that any analysis to establish the adequate level of protection should focus on two basic elements: one, the content of the applicable standards and two, the means to guarantee its effective application.

The Article 29 Working Party identified six basic substantive principles of data protection and three basic procedural requirements, whose compliance could be considered a minimum requirement for protection to be considered adequate. The substantive principles of are: the principle of limitation of purpose, the principle of data quality and proportionality, the principle of transparency, the principle of security, the rights of access, rectification and opposition, and restrictions on subsequent transfers. The 1998 working document also lists three additional principles for certain types of processing: confidential data, direct marketing, and automated individual decision. The principles of procedure are: to provide a good level of compliance with the rules, to provide support and assistance to individuals in the exercise of their rights, and to provide adequate reparation to the injured party.

As mentioned in the introduction, just a few countries have been recognized by the EU as having an adequate level of protection. A study designed to determine the similarities of the countries recognized as having an adequate level of protection found that all of them had a general rule on the protection of personal data that incorporates the basic principles. Additionally, they all have sectoral provisions for the treatment of some personal data. Specifically, 71.42 percent of the countries have acquired international commitments such as Convention 108 of 1981 and 42.85 percent, have a constitutional rule that refers to data

protection. Therefore, when analyzing the Colombian data protection framework it is important to verify that Colombia has these standards.[19]

2.3 General Data Protection Regulation

Provisions under Chapter V of the GDPR regulate data transfers from the EU to third countries, international organizations, and all data transfers. The DPD only provides for data transfer to third countries without reference to international organizations. A mechanism called "adequacy decisions" for such transfers remains the same under both laws. However, in situations where the Commission does not take adequacy decisions, alternate and elaborate provisions on "Effective Safeguards" and "Binding Corporate Rules" have been mentioned under the GDPR. Other specific situations have been envisaged under both the GDPR and DPD for data transfers in absence of adequacy decision. These are quite similar with only a few modifications.[20]

Significantly, the GDPR brings clarity with respect to enforceability of judgments and orders of authorities that are outside of the EU over their decision on such data transfers. Additionally, it provides for international cooperation of the protection of personal data. These are not mentioned in the DPD.

Article 45 of the GDPR and Article 25 of the DPD, establish that the EC can verify that a third country ensures an adequate level of protection, if a specific authorization by a data protection authority is not required for the transfer of personal information. Such decision may cover all or some specific categories of transfers, such as airplane passenger information. According to Recital 104 of the GDPR "(…) the third country should offer guarantees

[19] Nelson Remolina-Angarita, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010).

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 Last Accessed August 2017

ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors." This means that in order to be considered as having an adequate level of protection, the third country must guarantee minimum standards to rights and matters such as: explicit consent by the data subject, conditions for the processing of children's personal data, the right of data subjects to request erasure (right to be forgotten), data breach notification, independent data protection authority, and effective judicial redress mechanisms, among others.

Unlike the DPD, the GDPR expressly points out in Article 45 (2) the elements to be considered when determining adequacy as follows:

"(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments

as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."[21]

The Commission has mentioned that adequacy decisions are "living" documents, and therefore, once the Commission decides that a third country assures an adequate level of protection, it must be monitored and subject to periodic reviews at least every four years, to determine that developments in its legal system continue to comply with the GDPR.

As mentioned in the introduction, it would be very ambitious and practically impossible to make a detailed analysis of the entire Colombian legal framework on data protection in relation to the GDPR in words limitation. The GDPR alone has approximately 60,000 words, not including the Colombian Main Data Protection Bill, sectoral laws, and relevant constitutional court rule of law. Therefore, the most relevant aspects of the Colombian legal system that should be considered by the Commission when making the assessment will be presented below. Through analysis of these aspects, one may be able to predict if the Colombian data protection framework could be recognized by the EC as having an adequate level of protection.

3. COLOMBIAN DATA PROTECTION FRAMEWORK

3.1 Background

Colombia established habeas data as a fundamental right when it was included in its 1991 Constitution. Article 15 of the Colombian Constitution states the following:

> All people have the right to their personal and family privacy and to their good name, and the State must respect them and protect them. Likewise, they have the right to know, update, and rectify the information that has been collected about them in data bases and in the files of public and private entities.
> In the collection, treatment and circulation of data, freedom and other guarantees enshrined in the Constitution will be respected.

[21] Article 45 (2) GDPR

> Correspondence and other forms of private communication are inviolable. They can only be intercepted or registered by judicial order, in the cases and with the formalities established by law.
> For tax or judicial purposes and for cases of inspection, surveillance, and intervention by the State, the presentation of accounting books and other private documents may be required, under the terms established by law.[22]

At the time, data protection was reflected in case law development of the Constitutional Court, which through landmark judicial decisions was developing several principles and giving remedies on a case-by-case basis.[23]

In 2008, the National Government considered that it was necessary to issue a comprehensive data protection law, which establishes all the principles and mechanisms to exercise people's rights. Therefore, the National Congress issued Law 1266, projected to be a general rule for data protection. However, The Colombian Constitutional Court in its revision determined that the law did not correspond to a general data protection law, but rather, sectorial data protection provisions focused on just financial and credit services. It did not apply in other areas where personal data is normally handled. Hence, Colombia was lacking a general data protection law which covered all important aspects of the field in accordance with the European standard.

Law 1266-2008 ('Law 1266'), reviewed by the Colombian Constitutional Court in Decision C-1011/2008, regulates the collection, use, and transfer of personal information regarding monetary obligations related to credit, financial, and banking services.

Law 1581 of 2012 (Colombian Data Protection main regulation), reviewed by the Colombian Constitutional Court in Decision C-748-2011, contains comprehensive personal data protection regulations. Accordingly, Law 1581 applies to personal data stored in any public or private database or file, any processing treatment of personal data in Colombia, and

[22] Article 15 Colombia Constitution
[23] Several Judgments created principles and rights.

operations performed by individuals who are not located in Colombia but are subject to the jurisdiction of Colombian Law under international standards and treaties.

Under Law 1581, the data subject must always give prior, expressed, and informed consent for all activities pertaining the collection, use and transfer of personal data, except those that are specifically exempted from all or part of the Law, which includes the processing of credit data under Law 1266. Decree 1377 of 2013, which constitutes secondary regulation on data protection matters, regulates more detailed issues regarding the authorization given by data subjects for personal data treatment including sensitive data. It also regulates subjects such as measures to be implemented regarding data collected before the publication of the Decree, policies on processing treatment of personal data, the exercise of data owner's rights, cross border transfer and transmission of personal data, and liability regarding the processing of personal data through the organizational implementation of the accountability principle[2425].

An important aspect to take into account when analyzing the Colombian legal system and any specific fundamental right, are the binding decisions of the Constitutional Court on the matter. Although the Colombian system is framed by a civil law tradition, from the Constitution of 1991 with the creation of the Constitutional Court and its multiple sentences, the concept of the judicial constitutional precedent that has been incorporated into the legal system is very similar to the one adopted in common law countries[26].

Therefore, it is very important to analyze the rules in light of the jurisprudence of the Constitutional Court, since some judgments have *erga omnes* effects or have established a rule of law. In some judgments, the Court has created rights or repealed norms because they are not compatible with fundamental rights. For instance, the right to be forgotten has been a jurisprudential creation in Colombia that is not found in any law. Since its inception, the Court has been very proactive in its decisions on data protection, so it is very important that

[24] Articles 6, 9 of Law 1581 developed consent of data subject.
[25] Article 10 of Law 1581 point out the exceptions regarding data subject's consent
[26] LÓPEZ MEDINA, Diego Eduardo, El derecho de los jueces, 3a. reimp., Bogotá, Legis-Uniandes, Facultad de Derecho, 2002.

the EC take into account the jurisprudence of the Constitutional Court when making the assessment for adequate level of protection[27].

3.2 Constitutional Court and Preferential Fundamental Rights Action

The Constitutional Court issues three kinds of sentences. The first of these, Sentence T (Tutela), analyzes sentences issued by inferior judges chosen for their constitutional relevance and that have been lawsuits filed by citizens (Tutela Action) because they consider that their fundamental rights have been undermined. As a general rule, these sentences have inter-party effects, however, sometimes a certain Rule of Law is created that must be observed and applied by judges. The second, Sentence SU (Unified Sentence), analyzes several T sentences issued by lower judges chosen for their constitutional relevance and decided in a single sentence. This sentence has *erga omnes* effects and usually creates a rule of law. The last, Sentence C (Constitutional Sentence), issues decisions on whether or not a rule is in accordance with the Constitution. These sentences have *erga omnes* effects and sometimes repeal norms, clarify, or interpret the scope of such norm. Therefore, through these three types of sentences, the Court has issued important decisions regarding the Colombian data protection framework, which must be analyzed in conjunction with the existing regulations.[28]

Among the constitutional redress mechanisms created by the Colombian Constitution, the most used by citizens seeking to protect their data protection rights is the "Tutela Action." Under this action, citizens can file a lawsuit before any Judge of the Republic through a preferential judicial process. The Judge must reach an immediate compliance decision within the next ten business days. The sentence can be appealed and its final decision will be known within the next 20 days. For this agile procedure it is not necessary to seek the services of a lawyer and it has become an effective judicial action for the defense of fundamental rights in

[27] Ibid.
[28] http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-05792000000100004 Last accessed July 2017

Colombia. Through this type of sentence, the Constitutional Court has established rules and has assigned binding interpretation to the data protection regulation.[29]

In Colombia data protection, fundamental right was developed by the Constitutional Court from its beginnings under the terms "IT freedom" and "informative self-determination." In judgment T-414 of 1992, the Court indicated that:

> The possibility of accumulating information in an unlimited quantity, of confronting and gathering it, of tracking it in an indefectible memory, of objectifying it, and transmitting it as merchandise in the form of tapes, rolls, or magnetic disks, for example, allows a new power of social domain over the individual, the so-called computing power. As a necessary counterweight, this new power has engendered 'IT freedom.' It consists of the faculty of disposing of information, of preserving one's own identity, that is, of allowing, controlling, or rectifying data concerning the personality of the holder thereof and, as such, identify them before the rest. It is, as we can see, a new social dimension of individual freedom, and because of the circumstances that explain its appearance, of other classic manifestations of freedom.

Sentence T-414 of June 16, 1992 was the first on the subject in Colombia, and perhaps one of the first in Latin America. Subsequently, Judgments T-008 of 1993 and T-022 of 1993 continued to refer to the subject in question and to other relevant aspects regarding the processing of personal data. Some concepts developed by case law have established the following:

- Creation of the Rule of Law in Colombia according to which in cases of conflict between the right to privacy and the right to information, as a rule "this Court does not hesitate to recognize the prevalence of the right to privacy over the right to information, it is a necessary consequence of the consecration of human dignity as a fundamental principle and essential value of the social State of Law in which Colombia has been transformed today, according to Article 1 of 1991 of the Colombian Constitution."[30]

[29] Decree 2591 of 1991 regulates this matter.
[30] Colombian Constitutional Court Judgment T-414 of June 16, 1992

- Creation of the Rule of Law according to which is the data subject owner of the personal data and not the administrator or owner of a database in which that type of information is inserted.

- Incorporation in Colombian jurisprudence on concepts of computer freedom, habeas data, constitutional computer law, prison of the soul, profiles of virtual people, and the right to be forgotten (expiration of negative personal data).

- Establishment of the need for prior authorization of the data subject as a requirement for the processing of personal data and the respect of "due process" and the responsible use of information technology[31].

Constitutional jurisprudence has also established the following principles: the effectiveness of the full protection of human dignity, and technological progress can not harm human rights and freedoms.

Subsequently, the Constitutional Court has referred to on several occasions "IT self-determination" and has established the scope and the essential core of the right of habeas data as one of the innovations of the 1991 Constitution and as a "fundamental" guarantee.

The Court itself has recognized the different meanings of this right which ultimately has been classified as one of a fundamental and autonomous nature. The first jurisprudential line interpreted the right to habeas data as a guarantee to the right to privacy. The second line of interpretation considered habeas data as a manifestation of the free development of personality. In 1995, a third arose that currently rules that habeas data is understood as an autonomous right. According to Judgment SU-082 of 1995:

> The core of the right to habeas data is composed of computer self-determination and freedom -including economic freedom-. In addition, this right includes at least the following prerogatives: a) The right to know the information that refers to it; b) The right to update such information; c) The right to rectify information that does not correspond to the truth, and

[31] Ibid

includes the right to erasure the negative data. In Sentence T-176 of 1995, the Court indicated that the right to habeas data is undermined when one of the prerogatives stated in Sentence SU-082 of 1995 is threatened.[32]

The importance that Latin American constitutions have conferred on data protection is indicative of the desire that in the region people be adequately protected from the undue treatment of their personal data. That is why the constitutions have consecrated, in a progressive and cumulative way, a series of rights and duties that must be fulfilled by those responsible for the treatment of personal data. Additionally, there are constitutional legal actions that allow people to demand their rights[33].

The constitutional construction of the fundamentals of data protection in Colombia is visible in many judgments of the Court in which a series of principles were developed that are mandatory. These principles, at the same time, have been the backbone of some sectoral regulations, and of Law 1581 of 2012.

4. COLOMBIAN DATA PROTECTION REGULATION (Law 1581 2012)

4.1 A close relation with European Data Protection Directive

Although the development of the Colombian Constitutional Court in terms of data protection has been a positive and abundant initiative, it was necessary to issue a General Law of constitutional rank that could encompass all the rights and principles in a comprehensive manner. Through these actions, Colombia also sought to have regulations on data protection that were on a par with international instruments such as those defined by the EU.

[32] Judgment SU-082 of 1995

[33] The majority of Latin-American countries has established Data Protection as a fundamental right. For instance, Colombia (Article 15), Mexico (Article 6), Argentina (Article 43), Panamá (Article 42), Bolivia (Article 130), Brazil (Article 5), among others.

The first attempt was Law 1266 of 2008, but the Court determined that this law only corresponded to a sectoral regulation for financial and banking matters. For this reason, it was necessary to issue Law 1581 of 2012, which was referenced by the European DPD. However, it is important to remember that the Court interpreted the law and made some clarifications through Judgement C-748 of 2011.

The Constitutional Court stated, in relation to the European Data Protection framework that:

> (...) these standards are not mandatory for the Colombian State, but they are a valuable source for the constitutional judge when making a decision, because precisely what is intended with the project under study, in addition to achieving a protection of the personal data in the terms required by the Constitution, is to ensure that the country complies with international standards in the objective to achieve certifications necessary to enter the market, as a territory with adequate levels of protection of personal data. [34]

The European DPD has such a close relationship with Law 1581 of 2012 that it even has a similar number of articles and regulates the field of data protection in a very similar way. Therefore, the Colombian law encompasses the same principles, rights, and obligations as the DPD in a general way and reference will be made only to some that deserve special comment.

4.1.2 Principles, Rights, Obligations Comments

Law 1581 of 2012 intended to regulate Articles 15 and 20 of the Constitution. However, the Constitutional Court concluded that this law "only indirectly develops the rights to privacy, good name, and information, that is, it cannot be considered a total and systematic regulation of such rights."[35]

With respect to Article 15 of the Constitution, the right of all persons to know, update, and rectify the information that has been collected about them in databases or files was regulated, along with some issues related to the collection, treatment, and circulation of said

[34] Judgement C-748 of 2011.
[35] Ibid.

information. With regard to the right to information, only aspects related to the quality of information were mentioned. Therefore, Law 1581 is not an integral and complete regulation of the aforementioned constitutional articles[36].

The Court said that the provisions of Article 1 of Law 1581 are not the only constitutional guarantees that include the right to habeas data because "the powers to know, update, and rectify are not the only ones, but also others such as authorizing the treatment, including new data, or excluding or deleting them from a database or file. Therefore, although the norm is compatible with the Constitution, it should not be understood as a restrictive list."[37]

Under Law 1581 and Article 3 of Decree 1377, 'sensitive data' is data that is related to the intimacy of the data subject, or that, if disclosed without consent, could lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, trade-union membership, social organizations, human rights organizations, or those organizations that promote the interests of any political party or that ensure the rights and guarantees of opposition political parties, as well as data relating to health, sexual life and biometrics. Like the comments made on the scope of the Law, the Court noted that although the norm is compatible with the Constitution, it should not be understood as a restrictive list.[38][39]

The prior expressed and informed authorization of the data subject is the enabling legal support that will allow the processing of sensitive data for relevant purposes. In cases where by in law it is stated that the authorization of the data subject is not necessary, such law should indicate the purpose of the treatment and be consistent with the principle of proportionality. The authorization of the data subject is not required in the following cases: data required by a court order, data related to medical emergencies, data related to scientific purposes, and data related to the Civil Registration of Persons.[40]

---

[36] Ibid
[37] Ibid
[38] Ibid.
[39] http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf Last Accessed November 2018
[40] Ibid

In some international documents it has been considered that processing is legitimate when it refers to sensitive data that "the data subject has made manifestly public.[41]" However, the Constitutional Court declared the nullity of this exception under the argument that sensitive data does not become public data only because the owner or data subject makes it known to the public. Therefore, in this aspect the Colombian legal framework turns out to be more protectionist for the data subject than those documents.[42]

4.2 Analysis of GDPR Particularities

4.2.1 Right to be forgotten

Article 17 of the GDPR established what is commonly known as the "right to be forgotten" and its inspiration is based on a CJEU landmark decision that forced Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information. However, it is important to note that this right is not absolute and that it can be accessed under certain requirements[43].

In Colombia the negative information, as a rule by jurisprudential creation, should not be maintained indefinitely. Taking into account the above, the Constitutional Court has recognized the validity of the principle of expiration of negative information, which implies that personal information unfavorable to the data subject must be removed from the databases following criteria of reasonableness and timeliness. The Court stated that: "It has been jurisprudence of this Court that the negative and hateful information to the name of a person, is subject to a term of expiration under the idea of its limited permanence in time."[44]

---

[41] Article 3 Latin-American Data Protection Guidelines of 2007
Article 9 (e) GDP

[42] Colombian Constitutional Court Judgment C-748 of 2011.

[43] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Case C 131/12

[44] Colombian Constitutional Court Judgment Judgment T-414 of 1992

Since Judgment T-414 of 1992, the Court has held that personal data has limited validity, and "cannot have the character of being unmodifiable, and that negative data cannot be turned perennial or remain indefinitely." Thus, for example, in criminal matters, the Court has specified that "the data on the cancellation of an arrest warrant must disappear as soon as the competent judicial authority so orders or has certified that prescription has operated".

In Judgment T-022 of 1993, the Court established that once the purpose of the process is satisfied, the cancellation of the data can be requested and that, "this must be total and definitive." For instance, financial institutions will not be able to transfer or store the data in a historical file when the full and final exclusion of the name of the petitioner is appropriate. Therefore, the Colombian Constitutional Court has created jurisprudentially "the right to be forgotten" because once the purposes of the process have disappeared, the negative data must be removed otherwise the negative information would have a vocation for permanence. However, the Court has clarified that the right to be forgotten is not absolute, so the particularities of each case must be analyzed through objective criteria.[45]

The Court has also made it clear that the permanence of negative data causes damage to the data subject because "it is evident that the permanence of the negative data causes, minute by minute, enormous damage to the person, for which it is undoubtedly contrary to the Constitution and highly offensive to the dignity of the individual."[46]

In Judgment SU 082 of 1995 with *erga omnes* effects, the Court mentioned that the right to be forgotten is not expressly enshrined in Article 15 of the Constitution, but that it is deduced from the same article analyzing IT self-determination, and also from IT freedom principles. Therefore, this right of the data subject exists in Colombia and is protected by the Court through the mechanisms of judicial redress, especially, the constitutional "Tutela Action".[47]

[45] Judgment T-022 of 1993
[46] Ibid
[47] Judgment SU 082 of 1995

In Judgment T-063A/17 in October 2017, the Court ordered Google Inc. as owner of "Blogger.com" to remove the blog with address http://muebles-caqueta.blogspot.com.co as its content imputes anonymously unproven information on the commission of the crime of fraud and other expressions that can be considered insults and slander against the plaintiff and his company.

However, Google filed a nullity action because the Court failed to study and analyze arguments of constitutional relevance to which the Court agreed in May 2018 and to date it is again deciding on the merits of this matter. This nullity action filed by Google does not occur frequently and applies only exceptionally. Although the Court is deciding the case again, it does not necessarily mean that the decision will be completely different. Specifically, the Court is analyzing issues of jurisdiction and computer technical measures to decide again in depth. Consequently, the decision of the Court will soon be known and will surely be a landmark decision in the relationship between technological tools for Internet search engines and right to privacy.[48]

4.2.2 Children Rights

Concerning the protection of children's personal data, Article 8 of the GDPR requires parental consent for the processing of children's data, specifically for minors under 16. However, member countries may reduce the required age to 13.[49]

Meanwhile, Article 7 of Law 1581 of 2012 provides specific considerations regarding the processing of children's personal data. First, it reiterates the prevailing nature of their rights, which means that in the event of a possible conflict of rights, the protection of children will be preferred. Any measure or norm must prioritize the best interests of the rights of children. Secondly, it obliges the State to train children as citizens aware of the respect for their rights

[48] Judgment T-063A/17
[49] Article 8 of the GDPR

and those of others. Finally, it establishes that the processing of children's personal data is prohibited, except for the data that is of a public nature. This absolute prohibition was clarified by the Court, interpreting that the data of the children can be processed as long as the prevalence of their fundamental rights is not put at risk.[50]

Taking into account the above, in Article 12 of Decree 1377, some special requirements for the processing of personal data of children and adolescents were implemented. Among the requirements is the declaration that it is the decision of the legal representatives of the children to grant the authorization and, when appropriate, to take into account the opinion of the children depending on their individual maturity, autonomy, and ability to understand the matter.[51]

Therefore, the Colombian data protection framework contains specific and special regulations for children. In fact, it can be established that the Colombian law is more protectionist than the GDPR in this context, since it establishes the age of 18 years while the GDPR establishes 16 years.[52]

4.2.3 Notification Data Breach

According to Article 33 of the GDPR in the case of a personal data breach, the controller must notify the supervisory authority within the following 72 hours after discovering such event. If the notification is not made within the required time, a reasonable justification must be presented to the supervisory authority.[53]

Under Colombian Law, Article 17 (n) of Law 1581 requires that the data subject and the Colombian Data Protection Authority (hereinafter "CDPA") are notified in the case of security risks or violations of security policies related to the management of personal data.

[50] Article 7 of Law 1581 of 2012
[51] Article 12 of Decree 1377 of 2013
[52] Ibid
[53] Article 33 of the GDPR

Although the law does not indicate a specific procedure or period of time to notify a personal data breach, it must be done within a reasonable period of time according to guidelines of the CDPA.[54]

The CDPA has also established the minimum content that the communication of the data controller must have in the case of a data breach as follows: type of incident, date of the incident, date on which the Controller discovered the incident, cause, type of personal data compromised (sensitive, private etc), and the number of data subjects whose data was compromised.[55]

4.2.4 Privacy by Design And Default

One important change brought by the GDPR in Article 25 is the establishment of the principles of Privacy by Design and Privacy by Default. Colombia has not regulated the above *principles* in its legislation, which means not being in accordance with the GDPR is an obstacle to obtaining the EU's verification of having an adequate level of protection.

However, in 2017 a draft bill was filed before the Colombian Congress, to regulate aspects that do not exist in the Colombian data protection framework in accordance with the GDPR. Article 3 of the Draft establishes that:

> Principle of data protection from the design and by default. Before the processing of personal data is initiated and while it is processed, preventative measures of various kinds must be adopted (technological, organizational, human, procedural) to avoid violations to the right to privacy, as well as security flaws or the improper processing of personal data. Privacy, due processing of personal data, and the Security must be part of the design, architecture, and configuration predetermined by any technology or process of information treatment. Mechanisms will be used to ensure that, by default, only the data necessary to fulfill a specific purpose is processed and is done in a way so that personal data is not accessible to an indefinite number of people.[56]

[54] Article 17 (n) of Law 1581 of 2012
[55] Ibid
[56] http://progresomicrofinanzas.org/wp-content/uploads/2017/11/colombia-pl-089-17-habeas-data.pdf Last Accessed December 2017

The draft is currently being considered and it is expected that soon it will be adopted as law.

4.2.3 Data Protection Officers

Articles 37, 38, and 39 of the GDPR [57]introduce a new requirement to organizations which must appoint a data protection officer (DPO) in their internal structure. Rights, obligations, and tasks of the DPO are clearly laid out in the GDPR and are in line with those established in Colombian regulation.

It is important to highlight that Colombian main Data Protection Bill does not require organizations to appoint a DPO. However, Decree 1377 does require organizations to appoint a person or area that will assume the responsibility of personal data protection matters and that will process the exercise of the rights of the data subjects. The requirement of such position has also been included in the accountability guidelines issued by the Colombian Data Protection Authority "CDPA" on May 2015. Two articles of Decree 1377 refer to DPO as follows:

Article 23, Decree 1377 of 2013. "All responsible persons in charge must designate a person or area that assumes the function of personal data protection, which will process the requests of the data subjects, for the exercise of the rights referred to Law 1581 of 2012 and this Decree."

Article 27, Decree 1377 of 2013. "Effective internal policies. In each case, according to the circumstances mentioned in numerals 1, 2, 3 and 4 of Article 26 above, the effective and appropriate measures implemented by the Responsible must be consistent with the instructions given by the Superintendence of Industry and Commerce (CDPA)."

The CDPA recently defined the concept 17-145072-2, which states that:

> "(…) the function of the data protection officer or the area responsible for data protection in the organization is to ensure the effective implementation of the policies and procedures

[57] Articles 37, 38, and 39 of the GDPR

> adopted by it, to comply with the rule of protection of personal data, as well as the implementation of good personal data management practices within the company. The personal data protection officers will have the task of: (i) structuring, designing, and managing the program that will allow the organization to comply with data protection regulations, (ii) establish the controls for that program, its evaluation, and permanent review."[58]

Therefore in Colombian data protection regulation, it is mandatory to appoint a DPO with similar obligations or tasks as are established in the GDPR. Normally Colombian organizations appoint legal departments or lawyers to act as DPOs, but their role has recently become more active.

4.2.4 Accountability

The Accountability principle is one of the main changes introduced by the GDPR. Article 24 of the GDPR requires organizations to implement "appropriate technical and organizational measures" to be able to demonstrate their compliance with the GDPR, which shall also include the implementation of appropriate data protection policies. Therefore, organizations will have to implement not only internal and publicly-facing policies, records and notices, but also technical measures, and fundamental personnel and strategic changes to their processing operations.[59]

With the 1581 Law, Colombia became one of the first countries to have enshrined the accountability principle in its national data protection law and to impose mandatory accountability obligations on private and public sector organizations. Decree 1377 of 2013 requires data controllers and data processors that collect or process personal data of individuals who reside on Colombian territory to comply with the accountability principle.

The Colombian regulation of the accountability principle is very much aligned with the approach adopted by the Article 29 Working Party in its Opinion 3/2010 and obligations established later by the GDPR.[60]

[58] Colombian Data Protection Supervisory Authority concept No. 17-145072-2
[59] Article 24 of the GDPR
[60] Article 29 Working Party in its Opinion 3/2010 and obligations

Article 27 of Decree 1377 of 2013 established that the effective internal Policies must: a) have an administrative structure proportional to the structure and size of the Responsible Company; b) adopt implementation tools, training and education programs, and c) adopt processes for the attention and response to requests submitted by the data subjects.[61]

Therefore, in 2015, the CDPA published the Accountability Guide in which it aims to establish minimum standards so that organizations can demonstrate that a data breach corresponds to an isolated situation according to the Comprehensive Personal Data Management Program. The CDPA established that such Program should contemplate at least the following:

1. Commitment to the Organization: financial and personnel resources must be allocated to implement the Program.
    a. From top management: the support and commitment of senior management is essential, for which a responsible area should be designated, as well as the allocation of sufficient resources to design and implement the program.
    b. Responsible for the protection of personal data: is the person who must guarantee the effective implementation of policies and procedures, as well as implement best practices; in addition to administering the Program as such.
    c. Reporting: establish internal reporting mechanisms to inform the monitoring and execution of the Program, as well as implement internal audit plans that allow compliance monitoring.

2. Program controls: once the process of due diligence within the organization has been advanced, controls must be developed to allow the Personal Data Protection Officer to develop the Program:
    a. Operational procedures: administrative procedures to properly handle the inherent risks of the processing of personal data.

[61] Article 27 of Decree 1377 of 2013

b. Inventory of databases with personal information: to know what data is stored, how it is used and if they really need it, taking into account the purpose.
c. Policies: generates internal policies about what must be documented: the collection, storage, use, circulation, and elimination of personal data.
d. Risk management systems associated with the treatment: according to the type of organization, systems must be established to identify, measure, control, and monitor all the facts that put compliance with data protection regulations at risk.
e. Training and education required: of all employees and specialized training for those officials who handle personal data.
f. Response protocols in the handling of violations and incidents: management component that allows the identification of vulnerabilities and concentrate resources on mitigation measures. In the same way, there must be mechanisms that allow the presentation of internal reports and the incidents that must be reported to the Owners and the SIC.
g. Management of those responsible for processing the international transmission of data: provisions that include that the Administrators comply with Colombian regulations.
h. External communication: develop a procedure to inform the Holders of their rights.[62]

The Comprehensive Personal Data Management Program must also guarantee mechanisms to supervise, evaluate, and review it in a way that ensures its effective and pertinent implementation, for which it will be necessary to: i) Develop a plan for supervision and review that the DPO must take in consideration, and ii) Evaluate and review the program's

[62] http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf Last Accessed on July 2018

controls through continuous monitoring. Based on the results of the evaluation, the DPO should take the necessary steps to review and update the controls.[63]

The implementation of the measures mentioned in the guide will allow the organizations to demonstrate before the data subjects and the CDPA the adoption of a Comprehensive Personal Data Management Program, as well as the due diligence in the personal data process.

4.2.5 Judicial Redress Mechanisms

Data subjects have many judicial mechanisms for the protection of their data privacy rights within the Colombian legal framework. As mentioned in Chapter 3.2, any natural or legal person has the right to file, before any Colombian judge, a special constitutional lawsuit, referred to *as "Acción de Tutela"* in Spanish in order to exercise any of their fundamental rights such as: privacy, data protection, or habeas data, among others. Since the implementation of the Constitution of 1991, this redress mechanism has been the most used by citizens for the protection of their data privacy rights and has allowed the abundant jurisprudence of the Constitutional Court on the matter.[64]

This constitutional special protection is regulated by Decree 2591/91 and Constitutional Court judgments which expressly provide that "Tutela" Action can be filed against a private individual or company that undermines Article 15 of the Colombian Constitution. The Judgment which decides a "Tutela" lawsuit normally will issue a writ or order that must be obeyed within the next 48 hours after being notified of the decision. Failing to observe a Judge's ruling could result in an imprisonment order against the defendant for a period of up to 10 days, among other determinations.[65]

[63] Ibid
[64] Decree 2591 of 1991
[65] Ibid

Another mechanism used by the data subjects is the "right of petition" established in Article 23 of the Constitution and regulated by Law 1755 of 2015. This procedure consists of the direct claim by the data subject to the data controller or processor so that it respects its rights immediately[66]. If this does not occur within 15 days after the claim is filed, the data subject may file a "Tutela" action or a complaint before the CDPA.[67]

The CDPA is allowed to initiate administrative investigations by their own initiative or by data subject requests against those who breach the provisions of Law 1266 or Law 1581 and to impose penalties of up to 2,000 Minimum Monthly Legal Wages (approximately 500,000 dollars) for each case, and sanctions that include the temporary or permanent closure of the professional or commercial activities of the subject who breached the data protection regime. The penalties under Law 1581 only apply to private entities. If an offense is committed by a public entity, the Superintendence of Industry and Commerce shall refer the action to the Attorney General's Office to initiate the respective investigation.

The previous expedited judicial mechanisms are used by the data subject usually to obtain an injunction for the protection of their rights, but if a data subject wants a compensatory relief, he can file a civil lawsuit before a civil judge in accordance with Colombian General Procedural Code. To date there is no known case of a lawsuit whose claims include compensatory relief due to a data breach, but the legal system allows it.

Also, the Colombian legal system allows that a plural number of data subjects can file collective actions. According to Article 88 of the Constitution and Law 472 of 1998, data subjects may file a popular action or a group action. Popular actions are designed to obtain an injunction while group actions are for a compensatory relief. The two legal mechanisms have particularities with the group action having greater procedural requirements. Although to date there is no known case law of a collective action regarding data protection, perhaps because the data subjects have exercised their rights directly and individually through the

[66] Articles 15 and 16 Law 1581 mentioned the possibility of this mechanism
[67] Law 1755 of 2015

"Tutela" Action, the Colombian legal system allows it. It is important to mention that the GDPR established in Article 80 that member states must guarantee protection in a group manner, a requirement that is fulfilled by Colombia.[68]

Additionally, on January 5, 2009, Colombia's Congress enacted Law 1273, which added an "Information and Data Protection" criminal offense to Colombia's Criminal Code. In particular, Article 269F states: "Violation of Personal Data: Anyone who, without being authorized to do so, to their own benefit or for a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies, or uses personal codes, personal data contained in files, archives, databases, or similar means, will be held liable for imprisonment for a term of forty eight (48) to ninety six (96) months and a fine." Therefore, a public prosecutor may, by his own initiative or request of a data subject, initiate criminal investigations of data controllers or data processors for the presumptive commission of crimes.[69]

4.2.6 International Transfer

Under Law 1581, specifically Article 26, the cross border transfer of data is prohibited unless the foreign country where the data will be transferred meets at least the same data protection standards (adequate level of protection) as the ones provided under Colombian law. This prohibition also applies to personal data governed by Law 1266. Adequate levels of data protection have been determined by the CDPA in External Communication 005 of August 10, 2017.

The prohibition against cross-border transfers does not apply if the data subject has expressly authorized the cross-border transfer of data, there is sufficient information regarding destination and usage, and the transfer falls into one of the following categories: the exchange

[68] Judgment C-215/99
[69] Act 1273 of 2009

of medical data bank transfers, stock transfers agreed to under international treaties to which Colombia is a party, transfers necessary for the performance of a contract between the data owner and the controller, or for the implementation of pre-contractual measures provided there is consent of the owner, and transfers legally required in order to safeguard the public interest.

In External Communication 005, the CDPA established a list of 36 countries (all GDPR Member States are included) that the entity considers to have an adequate level of protection of personal data, within which the US was featured as a novelty. Colombia is the first country in the world that has come to that conclusion. The European Union and other countries have decided that only a few companies in the US have an adequate level, as long as they meet certain requirements, but under no circumstances at the moment, the entire territory of the US. [70]

This decision has been criticized by academics, who have mentioned that the decision was not sufficiently studied or substantiated. The landmark CJEU Schrems case that determined that the US Safe Harbor did not comply with European standards, showed that there is some concern about the way in which the US regulates data protection. Although according to the communication, the CDPA can change its decision regarding any country, the fact that Colombia has decided that the US has a Colombian adequate level of protection could affect Colombia's odds of achieving the GDPR standard

4.2.7 Colombian Independent Data Protection Supervisory Authority

In Colombia there are currently two administrative authorities responsible for enforcing laws and regulations on privacy data protection: the Superintendence of Industry and Commerce; and the Financial Superintendence of Colombia. Two different governmental authorities were designated as data protection authorities by Law 1266: The Superintendence of Industry

[70] https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Circular_Externa_5_Ago_10_20177.pdf Last Accessed November 2018

and Commerce ('SIC') and the Superintendence of Finance ('SFC'). As a general rule, the SIC will be the data protection authority (CDPA), unless the administrator of the data is a company that performs financial or credit activities under the oversight of the SFC as set forth in applicable law. In this case the SFC will also serve as a data protection authority.

The Superintendence of Industry and Commerce (CDPA) is a technical body attached to the Executive Branch of the Public Ministry of Commerce, Industry, and Tourism, whose functions include compliance with consumer protection regulations, protection of personal data, compliance with antitrust regulations, management of the national system of industrial property, as well as jurisdictional issues related to consumer protection. Within this public entity, the Personal Data Protection Department will execute the processing of personal data. The CDPA has around 600 employees and its budget for 2018 was around 50 million dollars for its operations.[7172]

The Financial Superintendence of Colombia is a technical body attached to the Executive Branch of the Public Ministry of Finance responsible for supervising the functioning of the financial markets, among others, related to financial banks. As a data protection authority, it only has power within the financial sector.

Broadly SIC (CDPA) deals individually with the complaints that people present to it and depending on these claims, determines if the case merits the opening of an administrative investigation. However, it should be noted that the CDPA also has broad powers to issue instructions, perform external audit inspections, or conduct an official investigation on its own initiative.

The volume of claims handled by the CDPA in relation to data protection breaches or any violation regarding data protection is approximately 2,000 cases per year. One example of a case handled by the CDPA resulted in the fine of 140 million pesos imposed upon Linio's

[71] http://www.sic.gov.co/noticias/por-cuarta-vez-superindustria-sanciona-a-linio-por-no-respetar-derechos-de-titulares-de-los-datos-personales Last Accessed on August 2018
[72] http://www.sic.gov.co/ Last Accessed on August 2018

company for data protection violation. This violation was revealed by Felipe Garcia, former Superintendent in charge, at the beginning of the fifth Congress on Personal Data Protection held by the entity in June 2017, when he stated in his speech that:

> A citizen asked Linio to remove him from its database because he was receiving a lot of publicity and we issued an order to the company to comply with the request but it was denied, which is why the SIC imposed a fine of 140 million pesos. Garcia also revealed that: the highest penalty we have established has been 1,000 million pesos to a prepaid medical company a couple of years ago[73].

The CDPA also reported that since 2010, more than 700 fines have been imposed for the violation of personal data, for a value of 25,000 million pesos, around 9 million dollars. About 75 percent of the sanctions imposed by the entity are related to financial data breaches, especially reports to credit bureaus that do not correspond to reality, updating information in a timely manner, and the failure to notify the debtor before making a report to the risk centers. In addition, the CDPA stated that it has issued 1500 orders to correct, update, or eliminate information in the databases of companies[74].

Like the Uruguayan data protection regulation, Colombian Law 1581 created the National Register of Databases as a public directory of all database configurations operating in the country. This register will be managed by the SIC, and may be consulted by any citizen. The Ministry of Commerce, Industry, and Tourism enacted Decree 886 of 2014, as a secondary regulation to Law 1581. This Decree establishes the minimum content that must be included in any entry of databases registered with this National directory, and the terms and conditions of such registry, as well as the timing requirements for the registration of databases.

A data controller must record any database configurations that entail the processing of personal data in the National Registry. The following is the minimum information that must be included in the registry form: a) type of data, location, and contact info of the data controller; b) type of data, location, and contact info of the data processor; c) mechanisms

[73] Speech by Felipe Garcia, former Superintendent in charge, at the beginning of the fifth Congress on Personal Data Protection held by the entity in June 2017.
[74] Ibid

for data subjects to exercise their rights; d) name and purpose of the database's means of processing (manual and/or automated), and e) the data processing policy.

5. **2017 EUROPEAN COMMISSION COMMUNICATION**

5.1 Trade Relationship

The strongest commercial link between Colombia and the EU is the Free Trade Agreement –FTA- signed in June 2012, and enforced in 2013. The initial negotiations of this agreement were conceived within the framework of the Community of Andean Nations (CAN) but ultimately only Colombia and Peru reached an agreement. Therefore, the FTA was initially signed between Colombia, Peru, and the EU, but in 2016 Ecuador adhered to it as well after completing the negotiation step with the EU.

Of the four CAN member states, Colombia has the largest economy and is "the EU's fourth main trading partner in Latin America (…) For its part, the EU is the Colombia's second largest trading partner and the first source of direct foreign investment in the country."[75] Consequently, the EU – Colombia commercial relations have deepened, allowing both parties to focus binational initiatives on key areas for their economies. Matters such as fair trade, the responsible conduct of enterprises, sustainable development, and strengthening the agricultural sector are common objectives on the commercial agenda of both Colombia and the EU.

According to the former European Commissioner for Trade, Karel De Gucht, the Free Trade Agreement between The European Union, Colombia, and Peru allowed the European Union to "secure access to these markets for major offensive agricultural products and Processed

[75] https://eeas.europa.eu/delegations/colombia_en/15808/Colombia%20and%20the%20EU. Last accessed July 2018.

Agricultural Products."[76] Far beyond the goodness of the FTA for the promotion of exports/imports from both parties, this agreement also allows space for addressing issues that go beyond the commercial perspective but that might impact social welfare. For instance, issues such as the sustainable management of forest resources, the fight against illegal fishing, cooperation on climate change, and equal treatment in terms of working conditions,[77] are on the agenda of the bilateral committee for the permanent assessment of the agreement. Also regarding this agreement, it is important to note that since the implementation of the FTA, around 500 EU companies have settled in Colombia.

Even though most of the EU companies are dedicated to construction and development of infrastructure, IT companies (mostly Spanish IT companies) see Colombia as a technology reference for the region and the world, given its great infrastructure.[78] The last couple of years have witnessed an impressive emergence of IT companies and tech giants that have opened branches in Colombia because of its great potential for IT development. "Colombia is the third largest provider of technology services in Latin America after Brazil and Mexico with 2.5 billion dollars in revenue."[79] A majority of the new foreign investment projects in the sector come from Spanish and US companies.

The global economy trends now merge towards the IT sector and data exploitation. This is also a shared perspective for both the EU and Colombia. The EU aspires for the consolidation of a digital single market and Colombian efforts are focused in developing the *"Orange Economy."* Therefore, previous efforts for enhancing the commercial EU-Colombia relations

[76] http://trade.ec.europa.eu/doclib/docs/2010/march/tradoc_145896.pdf. Last accessed November 2018.

[77] https://eeas.europa.eu/sites/eeas/files/las_relaciones_economicas_y_comerciales_entre_colombia_y_la_union_europea._cinco_anos_de_implementacion_del_acuerdo_comercial_2013_2017_1.pdf Last accessed August 2018

[78] In fact, Colombia has extensive fiber optic coverage in addition to its 4G networks and important advances in satellite services and 5G technology.https://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-empresas-extranjeras-de-tecnologia-que-llegaron-a-colombia-en-2017-248180. Last accessed August 2018.

[79] https://www.forbes.com/sites/jeanbaptiste/2016/10/03/6-tech-companies-from-colombia-to-watch/#73daecb76cec Last accessed August 2018.

will facilitate the development of further links given the current economic trends based on the IT sector.

5.2 Key Location

Although there is not a direct geographical link between the EU and Colombia, they have a "particularly close historical connection thanks to political, trade, and cooperation dialogue covering bilateral, regional, and multilateral issues."[80] Particularly the political history and some Colombian cultural features are rooted in Spanish heritage, due to the colonization that took place between centuries XV and XIX.

At the end of the XIX century a flow of migrants from Germany, Italy, and Spain arrived to Colombia, and later, during the Spanish Civil War in the 1930s, Spanish people inhabited Colombia again. Although the number of migrants was not as significant as in other countries of Latin America, it is remarkable that many migrants occupied high positions in the Colombian society. Their presence influenced the political, economic, and cultural life of the by then, young nation, which allows us to understand the great coincidence of political values and legal systems between the EU and Colombia.

Particularly in the context of data protection, the Colombian framework has been inspired by the former Data Protection Directive, and Colombian legislative authorities are currently working on law drafts to be aligned with the current European data protection regulation – GDPR. Legislative alignment has been favored by the active role of the Spanish Data Protection Supervisory Authority within the Ibero-American Network for the Protection of Data, which provides advice on this matter to Ibero-American countries.

[80] https://eeas.europa.eu/delegations/colombia_en/15808/Colombia%20and%20the%20EU. Last Accessed July 2018

5.3 Important Regional Role

Even before the enactment of the Habeas Data (2012),[81] Colombia along with Argentina, Uruguay, and Chile has lead the emergence of comprehensive data protection regulation that aligns with the European perspective of privacy protection as a fundamental right.

The Colombian Data Protection Authority "CDPA" has been active in the development and enforcement of the data protection legal framework. Telecom companies such as Telmex and UNE were fined approximately 100.000 dollars each for reporting individuals either "for a period beyond the authorized term after the fulfilment of their obligations with the telecom companies, or for non-existing debts"[82].

Likewise, the protection of sensitive data has been granted to data that was not necessarily collected by electronic means. In 2014, "(the) stem cell bank Red Cord was fined for 70.000 dollars for the unconsented processing of personal data of women who tested positive for being pregnant in laboratory tests taken in a Bogota's lab"[83]

In the same sense, the CDPA keeps developing aspects of the general law in order to guarantee a consistent legal framework able to cope with the challenges imposed by technology. For instance, in 2015 the CDPA issued a writ similar to the Uruguayan law requiring all data controllers both private legal entities and partially owned corporations to register their database configurations by the end of 2016. In 2017, the CDPA set forth a

[81] This thesis has mentioned that although the Colombian Political Constitution of 1991 contains the right to privacy and intimacy, the early developments of a comprehensive regulatory framework for data protection dated back from 2008.
[82] https://globalcompliancenews.com/data-privacy/data-protection-enforcement-in-colombia/ Last accessed July 2018.
[83] https://globalcompliancenews.com/data-privacy/data-protection-enforcement-in-colombia/ Last accessed July 2018.

binding instruction guideline to assess the adequate level of data protection of a third country and the list of qualified third countries in which international data transfers can be done.

Unlike other Latin American countries, the Colombian jurisdiction included the right to be forgotten among the rights of the data subject as commented in Chapter 4.2.1. Case law related to the right to be forgotten has been approached from different perspectives in Latin American countries, including the Internet Service Provider –ISP- liability, the right to freedom of press, or merely by judicial order to block content in the absence of legal provision around this right.

Furthermore, the CDPA has performed investigative powers in international sounded cases such as *Cambrigde Analytica* -CA-. The investigation was against "Farrow Colombia SAS and Farrow Mexico who administered the application Pig.gi.2 and the CDPA temporarily blocked the application as a precautionary measure while the investigation was carried out"[84].

5.4 Political Relationship

Since the mid-1990s, political and economic ties have strengthened and materialized as a result of the signature of the Rome Declaration, the 2009 Memorandum of Understanding, and the Political Dialogue and Cooperation Agreement between the EU and the Andean Community. These political instruments paved the way to achieve constant political dialogue on relevant matters such as: climate change, protection of biodiversity and green diplomacy, the struggle against illicit drugs and related crimes, the promotion of human rights, and "since 2014, Colombia has had facilitated access to EU crisis management operations within the common security and defence policy."[85]

[84] https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175627/colombia. Last accessed November 2018.
[85] http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621834/EPRS_STU(2018)621834_EN.pdf Last accessed July 2018.

In the last years, bilateral cooperation and the constant dialogue between the EU and Colombia have resulted in both the Schengen Visa waiver for Colombian citizens in 2015, and the noteworthy participation of the European delegation in the peace talks with the FARC which ended in the signing of the Peace agreement with this armed group in 2016. Peace talks are underway now with the ELN (National Liberation Army) armed group and the EU has remained decisive in its commitment to support peace initiatives.

The active EU support of the implementation of the peace agreement is noteworthy. Both by the allocation of financial support and the growing presence of EU diplomats that oversee the process and provide resources for a variety of projects that span from the reconciliation process to psychological support for the victims of the conflict. Moreover, the European Commissioner for Human Aid and Crisis Management, Christos Stylianides, urged for the international community to keep supporting Colombia and added that Colombian people "can be sure that the European Union, together with the United Nations, will continue to be the strongest supporter of peace and human rights"[86]

From the regional perspective, Colombia has been a great ally for the EU in its initiative to develop a Euro-Latin American Parliamentary Assembly (EuroLat) in order to achieve a permanent forum for political dialogue with the Andean Community of Nations (CAN).[87] Colombia and the other members of the CAN share the same interest and have backed international commitments fostered by the EU. For example, "Andean countries have taken an active part in defining and developing legal, policies, and institutional measures for environmental policy."[88] For instance, in the recent Paris Agreements, Colombia devoted significant importance to its international commitment for the reduction of its emissions even though it accounts only for 0.41 percent of the global emissions.

[86] https://eeas.europa.eu/topics/instrument-contributing-stability-and-peace-icsp/38369/colombia-eu-will-continue-deliver-political-and-practical-support-peace-process_en Last accessed July 2018.
[87] http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621834/EPRS_STU(2018)621834_EN.pdf. Last accessed September 2018.
[88] http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621834/EPRS_STU(2018)621834_EN.pdf. Last accessed September 2018.

Additionally, Andean countries signed international agreements on the protection of children, indigenous people, and labor rights, where the EU has been actively involved. Political figures of the European Union have recognized the efforts and commitments of the Colombian government to strengthen the dialogue on human rights. This sort of political support reflects the similarity of interests that both the EU and Colombia foster in the International agenda.

According to the EU Ambassador in Colombia, Patricia Llombart, Colombia is seen as a "stable, reliable partner, with whom we share values at a time of turbulence in the international arena. A partner with whom we can work on the multilateral and global agenda."[89] In consequence, the EU – Colombia relationship can be deemed as strategic and deeply rooted on the coincidence of democratic values, which exceeds the commercial aspect.

[89] http://www.elcolombiano.com/internacional/la-union-europea-no-esta-para-dar-lecciones-sobre-migracion-XJ9469132. Last accessed October 2018

CONCLUSION

Since 1991 Colombia has been developing its data protection framework, mainly through the Colombian Constitutional Court's jurisprudential development that has allowed for the basis of data protection regulation, particularly with Law 1581 of 2012. Most likely due to cultural and legal traditions, especially in Spain (Member State of the European Union and the EU General Data Protection Regulation), Colombian's data protection regulation has been inspired by the European legal framework, a pioneer in this field. In this way, Colombia has established data protection as a fundamental right in Article 15 of its 1991 Political Constitution, and from this article, the extensive jurisprudential or case law has been developed by the Colombian Constitutional Court.

Therefore, taking into account the closeness to the European Union and a more globalized world due to the rapid development of new technologies, Colombia understands the need to receive recognition as having an adequate level of protection according to the European Commission under Article 45 of the GDPR.

When making such assessment, European commissioners should take into account the principal data privacy legislation (Law 1581 of 2012), sectoral regulation, other Colombian regulation regarding redress mechanisms, and above all, the judgments of the Colombian Constitutional Court, since it has not only interpreted the laws in the matter, but has also created Rule of Law, or data subject rights including the right to be forgotten.

When searching for information and legal literature in English on this topic, all documents found indicated that Colombia does not have a right to be forgotten and this is not true. It is likely that because the Colombian legal system has Roman roots or civil law tradition, they might think that since there is no specific norm that regulates this matter, it simply does not exist. However, this deduction cannot be applied to Colombia, since the Colombian

Constitutional Court judgments have an almost identical approach to the decisions of the High Courts in common law countries. Therefore, it is important to analyze and study the Colombian data protection framework with relevant Colombian Constitutional Court judgments.

One of the aspects analyzed in the countries that have obtained recognition as having a European adequate level of protection is that they all have a principal law and sectoral regulation. Although Colombia was delayed in having this type of written regulation (2012), the most probable reason for this is that it was not an urgent issue for Colombia, precisely because of the binding development that the Colombian Constitutional Court has given it since 1991. The importance of having a European adequate level of protection in the field, and the negotiations of a Free Trade of Agreement with the EU that was signed in 2012, marked the need to issue a comprehensive data protection framework.

Another aspect is that 48 percent of the countries that have obtained that recognition by the EU, have established data protection as a fundamental right in their constitutions. Colombia has done so as well under Article 15 of its constitution, even though it is not an essential requirement. Although Colombia is not part of Convention 108 of 1981, which has been joined by 71 percent of the countries that have obtained the adequacy parameter, such Convention is an important resource, along with the European Data Protection Directive and the General Data Protection Regulation, for the interpretation of the Colombian data protection framework as it has been established by the Colombian Constitutional Court.

In general terms, the Colombian data protection framework encompasses the same principles, rights, and obligations, similar to the current GDPR, but is not identical. Unlike the GDPR, which uses an exhaustive or limited list for subjects with respect to data subject type of rights and sensitive data, Article 1 of Law 1581 of 2012 and Article 3 of Decree 1377 of 2013 of the Colombian legal system, rule that such subjects cannot be interpreted as a restrictive list by interpretation and judgments of the Colombian Constitutional Court. In this sense, I consider that the wider scope imparted by the Colombian Constitutional Court provides greater protection to data subject, since judges are not limited by law, and with the rapid

advance of technology they can assign protection where they consider to be any type of violation not foreseen by the legislator.

Furthermore, the exception in the GDPR on sensitive data processing, which was inspired by the European rationale and approved by the Congress of Colombia, refers to sensitive data as data that the subject has made manifestly public. This was declared void by the Colombian Constitutional Court in Judgment C-748 of 2011 under the argument that sensitive data does not become "public data" only because the owner or data subject makes it known to the public. Considering today's social networks such as Facebook, where people publish sometimes sensitive information about themselves, this exception may be dangerous for data subject rights, since it opens the door to the processing of such data without requiring the consent of the owner or data subject. Thus, in this aspect Colombian law is also more protective of the data subject than the GDPR.

The GDPR and Colombian law regulate children's data similarly as they both contain the DPO´s data breach notification requirement, accountability principle, and effective judicial redress mechanisms. It is important to emphasize that under Colombian law the age of children is up to 18 years, and under the GDPR it is 16 years.

On the contrary, the GDPR is more protectionist than the Colombian law with respect to privacy by design and by default, since the Colombian data protection framework does not regulate this aspect. However, it is important to mention that a draft bill is currently being debated in the Colombian Congress. Additionally, the Colombian law does not require the Data Protection Officer to set a deadline when making the data breach notification, a condition established in the GDPR. With regard to this last aspect, it is suggested that the Colombian Data Protection Supervisory Authority issue at least one additional standard or guideline to establish a deadline.

Similarly, as in the GDPR, under Colombian law the cross border transfer of data is prohibited unless the foreign country where the data will be transferred meets at least an adequate level of protection. However, in August 2017 the Colombian Data Protection

Supervisory Authority stated that the United States has an adequate level of protection under Colombian law, which might be a disadvantage to Colombian law when seeking recognition as having a European adequate level of protection.

Basically Colombia has two options in order to remedy that disadvantage: (1) to declare that the US does not have an adequate level of protection, similar to New Zealand's determination in order to achieve a European equivalency, or (2) to adopt determinations similar to the EU-US privacy shield after having declared the US Safe Harbor invalid because of the Schrems case. Despite having data protection regulations similar to Europe, Colombia may seriously compromise its odds of obtaining an adequate level of protection according to the EU, if it does not implement either of these two alternatives.

It would be unfortunate if after all the important and innovative development made by the Colombian Constitutional Court and effort by the Colombian Congress, Colombia does not achieve recognition as having a European level of adequate protection only because of a hasty decision made by the Colombian Data Protection Supervisory Authority. Therefore, it would be beneficial if academics and experts in the data protection field raised their voices in protest so the Colombian Data Protection Supervisory Authority becomes aware and changes its decision or takes action on the matter.

REFERENCES

STATUTES

Colombian National Constitution (Colombian National Congress 1991).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Trade for All Towards a more responsible trade and investment policy, COM(2015) 497 final,.

Convention 108 of 1981 of the European Council

Data Protection Directive

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Decree 1377/2013, Data Protection Sectoral Law (Colombian Government 2013).

Decree 886/2014, National Registration of Data Bases (Colombian Government 2014).

Decree 2591 of 1991

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , 95/46/EC (1995).

Draft Bill 089/2017 (Colombian National Congress).

External Communication 005 (Colombian Data Protection Supervisory Authority 2017).

General Data Protection Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

Law 1581/2012, Colombian Data Protection Regulation (Colombian Congress).

Law 1266/2008 (Colombian Congress).

Law 1755/2015 (Colombian Congress).

Law 1273/2009 (Colombian Congress).

COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) (2016).

JUDGMENTS

Judgment of the Court (Grand Chamber), 13 May 2014.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Case C-131/12

Judgment of the Court (Grand Chamber) of 6 October 2015.

Maximillian Schrems v Data Protection Commissioner.

Request for a preliminary ruling from the High Court (Ireland). Case C-362/14

Colombian Constitutional Court in Decision C-1011/2008.

Colombian Constitutional Court in Decision C-748-2011.

Colombian Constitutional Court Judgment T-008 of 1993.

Colombian Constitutional Court Judgment T-022 of 1993 .

Colombian Constitutional Court Judgment T-414 of 1992.

Colombian Constitutional Court Judgment T-414 of June 16, 1992 .

Colombian Constitutional Court Judgment SU-082 of 1995

Colombian Constitutional Court Judgment Judgment T-063A/17

Secondary Literature

Bygrave Lee Data Privacy Law: An International Perspective Published to Oxford Scholarship Online: April 2014

LÓPEZ MEDINA, Diego Eduardo, El derecho de los jueces, 3a. reimp., Bogotá, Legis-Uniandes, Facultad de Derecho, 2002

Nelson Remolina-Angarita, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010).

December 7th 2017 Reply letter from the Director of the Colombian Data Protection Authority, Dra. María Claudia Caviedes Mejía.

https://www.usatoday.com/story/money/2018/03/06/jeff-bezos-unseats-bill-gates-forbes-2018-richest-billionaires-list/398877002/ Last Accessed March 2018

https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data Last Accessed December 2017

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en Last Accessed May 2017

https://www.law.berkeley.edu/library/robbins/CommonLawCivilLawTraditions.html Last Accessed June 2017

http://europa.eu/rapid/press-release_IP-18-5433_en.htm Last Accessed September 2018

https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf Last Accessed September 2018

English Collins Dictionary. Available at: http://dictionary.reverso.net/english-definition/adequate%20level

http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=8101969 Last Accessed March 2018.

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf Last accessed July 2017

https://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 Last Accessed August 2017

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-05792000000100004 Last accessed July 2017

http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf Last Accessed November 2018

http://progresomicrofinanzas.org/wp-content/uploads/2017/11/colombia-pl-089-17-habeas-data.pdf Last Accessed December 2017

http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf Last Accessed on July 2018

https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Circular_Externa_5_Ago_10_20177.pdf Last Accessed November 2018

http://www.sic.gov.co/noticias/por-cuarta-vez-superindustria-sanciona-a-linio-por-no-respetar-derechos-de-titulares-de-los-datos-personales Last Accessed on August 2018

http://www.sic.gov.co/ Last Accessed on August 2018

https://eeas.europa.eu/delegations/colombia_en/15808/Colombia%20and%20the%20EU. Last accessed July 2018.

http://trade.ec.europa.eu/doclib/docs/2010/march/tradoc_145896.pdf. Last accessed November 2018.

https://eeas.europa.eu/sites/eeas/files/las_relaciones_economicas_y_comerciales_entre_colombia_y_la_union_europea._cinco_anos_de_implementacion_del_acuerdo_comercial_2013_2017_1.pdf Last accessed August 2018

https://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-empresas-extranjeras-de-tecnologia-que-llegaron-a-colombia-en-2017-248180. Last accessed August 2018.

https://www.forbes.com/sites/jeanbaptiste/2016/10/03/6-tech-companies-from-colombia-to-watch/#73daecb76cec Last accessed August 2018.

https://eeas.europa.eu/delegations/colombia_en/15808/Colombia%20and%20the%20EU. Last Accessed July 2018

https://globalcompliancenews.com/data-privacy/data-protection-enforcement-in-colombia/ Last accessed July 2018.

https://globalcompliancenews.com/data-privacy/data-protection-enforcement-in-colombia/ Last accessed July 2018.

https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175627/colombia. Last accessed November 2018.

http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621834/EPRS_STU(2018)621834_EN.pdf Last accessed July 2018.

https://eeas.europa.eu/topics/instrument-contributing-stability-and-peace-icsp/38369/colombia-eu-will-continue-deliver-political-and-practical-support-peace-process_en Last accessed July 2018.

http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621834/EPRS_STU(2018)621834_EN.pdf. Last accessed September 2018.

http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621834/EPRS_STU(2018)621834_EN.pdf. Last accessed September 2018.

http://www.elcolombiano.com/internacional/la-union-europea-no-esta-para-dar-lecciones-sobre-migracion-XJ9469132. Last accessed October 2018