TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Stefano Roggiero

ECUADOR AS A COUNTRY WITH AN 'ADEQUATE' LEVEL OF DATA PROTECTION

Master's Thesis

Program HAJM, specialization Masters in Law and Technology

Supervisor: Anni Säär, MA

Tallinn 2020

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 19995 words from the introduction to the end of the conclusion.

Stefano Roggiero ……

(signature, date)

Student code: a166984

Student e-mail address: stefanoroggierob@gmail.com

Supervisor: Anni Säär, MA:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

Ecuador is in process of issuing its first personal data protection law, which will remove it from the list of countries with a deficient or null data protection legal framework. In these times of exponential digitalization, the protection of personal data transferred and processed abroad has become a priority, in particular for the European Union, which have made efforts to encourage non-member countries to adapt and harmonize their data protection regulations. Ecuador is obliged by its international commitments to improve the legislation over data protection, then, this work aims to determine if the dispositions and principles of its project of law (considering it is approved) are equivalent to the GDPRs`, and if it is the case, analyze the possibility of been awarded with an adequacy decision by the European Commission. Considering the strict demands of the European regulation and Ecuador´s current political and legislative situation, it is a challenge to comply with several of the elements that the EC contemplates.

Keywords: data protection; GDPR; adequacy decisions; privacy; cross border transfer of personal data.

Abbreviations

DPD	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.
EC	European Commission.
EU	European Union.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Councill 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.
EEA	European Economic Area.
IT	Information Technology.
ICT	Information and Communication Technology.
APDPL	Argentinian Personal Data Protection Law.
LOPDP	Organic Law on the Protection of Personal Data.
BCR	Binding Corporate Rules.
Constitution	Constitution of the Republic of Ecuador 2008.
COIP	Ecuador Criminal Code; *Código Orgánico Integral Penal.*
LOT	Organic Law of Telecommunications.
TRCA	Telecommunications Regulation and Control Agency.
TSP	Telecommunication Service Providers.
PDNSL	Public Data National System Law.
DPA	Data Protection Authority

INTRODUCTION

Within the first days of September 2019, the British Broadcasting Corporation BBC revealed a personal data breach of more than seventeen million Ecuadorians; almost every single citizen, considering Ecuador has a population close to eighteen million people.[1] This news generated a domestic scandal forcing the government of Ecuador to take action.

As a consequence of this scandal, the Personal Data Protection Organic Law Project (LOPDP)[2] was proposed by the Presidency of the Republic to the Ecuador National Assembly[3] on September 19, 2019, of which its objective is to "regulate the exercise of the right to protection of personal data, informational self-determination and other digital rights in the processing and flow of personal data".[4]

At the time of writing this thesis the LOPDP is in process of discussion at the National Assembly before it becomes an enforceable Organic Law.[5] This will cause several amendments and reforms to other laws and regulations of minor hierarchy which arguably and essentially, enable companies to misuse personal information and do not require the high standard of security that sensitive data ought to have. Therefore, it is visible that the topic of this thesis is timely.

Presently the majority of states are a significant source of all sorts of information, including personal data. The processing of large data bases are vital in order to execute governmental administrative functions, which demand an optimization of the processes to ensure the thin line between protecting rights and the possibility of violating such rights, is not crossed.

Information and Communications Technology is significant for individual life style and the manner in which they interact within the society, becoming an elemental tool for the day to

[1] BBC: Data on almost every Ecuadorian citizen leaked. September 16, 2019. https://www.bbc.com/news/technology-49715478
[2] Proyecto de Ley Orgánica de Protección de Datos Personales. Memorando No. PAN-CLC-2019-0184. Quito D.M, 19 SEP 2019.
[3] Ecuador National Assembly. Legislative Power of the Republic in charge of the creation of laws. https://www.asambleanacional.gob.ec/es
[4] LOPDP
[5] Organic Law: Law that is derived directly from the Constitution and serves for its best application.

day development in most aspects, such as work or studies. The emerging new technologies aim to personalize the products humans use based on their needs, the information they provide and using technology in as many opportunities as possible to make their life easier. As a consequence, technologies are covering almost all fields where people interact or develop, such as education, traveling, economy, law or art, for instance.[6]

Without a doubt the intention of new technologies, and the use of them, is to benefit or improve peoples' lives. However, it has become well-known in everyday life, that new technologies pose a high risk for illicit activity, and may be lucrative for criminals. This means that peoples' interaction with technology and personal data sharing presents a high risk if they are not aware of its value.

The topic of this paper was chosen as in the current day, when personal data flows from one place to another with ease, Ecuador does not have a law for the protection of the said personal data. Despite multiple complaints and public scandals regarding personal data misuse, not only at a governmental level, but also –and especially- in the private sector, in the year 2020 the law project is still under discussion. It is necessary to be aware of the importance of the influence and relevance that information and communication technologies and data analysis processes have. From the author's personal experience, it is common to hear, especially in Ecuador, stories where personal rights are affected due to the misuse of personal data, such as databases hacks or the sale of personal information stored in these data bases.

The purpose of this work is to expose the General Data Protection Regulation (GDPR) requirements that the European Commission (EC) considers in order to determine if non-member countries have an adequate level for the protection of personal data; and to review the current legal framework for the protection of personal data in Ecuador including the LOPDP. In doing the aforementioned, determine if Ecuador would able to meet the requirements of the GDPR and the EC, taking into consideration the existing practice based on adequacy decisions of Argentina and Japan under the Directive 95/46/EC and the GDPR respectively. Argentina is placed as an example due to the similarities with Ecuador regarding its political constitution and Japan as it is a decision made under GDPR.

[6] Constitution 2008 Republic of Ecuador Motives.

In order to achieve the objective described above, it is primarily necessary to expose the background and the current situation of data protection and the cross border transfer of data in the EU. Secondly, it is significant to analyze the current situation of the Ecuadorian data protection regulations and propositions of the LOPDP. It is also necessary to analyze the data protection laws of the countries outside of the European Union that are considered by the European Commission to offer an adequate level of protection of personal data, and for the purposes of this work specifically, the regulations of the Argentine Republic.

After the review of the above-mentioned laws, the differences or gaps between the content of the LOPDP and the EC considerations to determine an adequacy level of personal data protection can be exposed.

In order to establish the legal gaps between the Ecuadorian Data Protection Project and the legal requirements to be compliant with the GDPR, based on the European Commission decision over the Argentina data protection regulations, it was necessary to apply qualitative research.

Methodical and structured research leads to comprehend the legal concept of data protection and the transfer of such data. This works analyzes how distant the Ecuadorian Data Protection Project or LOPDP is to being considered as offering an adequate level of data protection according to the European Union standards imposed by the Article 45 of the GDPR.

The present regulations which give some sort of protection of personal data in Ecuador are analyzed by means of giving a clear account of the prevailing legal situation. Exploratory research is conducted, however the conclusion is a result of the legal assessment on what the legal differences are between the LOPDP and the requirements of the European Commission in order to issue an adequacy decision for a non-member state.

The materials considered and analyzed to accomplish the legal evaluation of the Ecuadorian, Argentine and European regulations on personal data, are academic articles, information in the public domain and news articles.

For the purpose of this work, other than the LOPDP proposed to the National Assembly, the Ecuadorian regulations reviewed are the Constitution of the Republic, international treaties

and national legislation. There are several differing laws that include dispositions which give personal data a legal status, but there is no one unifying data protection law in Ecuador as there is in the European Union or in Argentina.

The hypothesis of the work is: "Ecuadorian data protection regulations should be amended in order to meet the GDPR requirements in order to have an 'adequate' level of data protection and transfers on the basis of an adequacy decision". Although Ecuador has submitted the LOPDP project, the content it has might be not compliant with the GDPR and perhaps includes dispositions that would presumably not be able to guarantee an adequate level of data protection. Consequently, in order to affirm or overrule the developed hypothesis, six research questions were laid down:

1. What are the restrictions for cross border transfer of Europeans personal data?
2. What does Article 45 of the GDPR require in order to determine that a non EEA country offers an adequate level of data protection?
3. What are the rights, obligations and liabilities that the current Ecuadorian Data Protection regulations prescribe?
4. How does Ecuador protect personal data in practice?
5. What are the conditions in Ecuador for transferring personal data to or from third party countries?
6. Is there a possibility to be recognized as having an 'adequate' level of protection of personal data under Article 45 of the GDPR if the Organic Law on Personal Data Protection is approved?

The novelty of this work can be supported by the necessity of having a data protection law harmonized with the European Union. In addition, there is not a considerable amount of academic articles regarding the lack of data protection in Ecuador. Moreover the timing is convenient, as the LOPDP is awaiting discussion in the National Assembly.

Having dispositions for the protection of personal data spread among different laws and regulations, might offer a certain level of protection and some mechanisms to claim rights, but these are not enough to ensure the protection of sensitive information or personal data at an international level, nor to guarantee the rights provided by the Constitution of Ecuador.

1. PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

Personal data protection and privacy have become of crucial importance now that technology and the transmission of information are part of the society system.[7] Despite the last years' technology development and the international transfer of data exponential growth, the protection of personal data had its first appearances in human rights discussions consolidating in the late 40s'. However, alongside the inclusion of data protection and privacy as a human right the regulations over these rights have been appearing among European countries.[8]

The protection of personal data is defined by Frits Hondius as "that part of the legislation that protects the fundamental right of liberty, in particular the right to intimacy in regard to the automatic or manual process of data".[9]

The Directive 95/46/EC of the European Parliament on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (DPD) defines Personal Data as: "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[10]

The Working Party[11] issued an Opinion regarding the definition of personal data, concluding the following:

"The Working Party's analysis has been based on the four main "building blocks" that can

[7] Hallinan, Dara; Friedewald, Michael; McCarthy, Paul. (2012) Citizens' perceptions of data protection and privacy in Europe. Computer and Law & Security Review Volume 28, p. 263

[8] Cate, Fred. H. (1995). The EU data protection directive, information privacy, and the public interest. Iowa Law Review 80(3), p. 431

[9] Hondius, Frits. (1983) A Decade of international data protection. "Netherlands of International Law Review", Vol. 30, No. 2 p. 105-106

[10] Directive 95/46/ Article 2.

[11] The Article 29 Working Party (Art. 29 WP) extinct advisory entity created of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. Replaced by the European Data Protection Board (EDPB) under the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

be distinguished in the definition of "personal data": i.e. "any information", "relating to", "an identified or identifiable", "natural person". These elements are closely intertwined and feed on each other, but together determine whether a piece of information should be considered as "personal data". [12] Nonetheless, according to Millard and Church the Working Party Opinion lacks recognition of the barriers and problems coming from a wide definition of personal data and moreover it does not take into consideration different approaches.[13]

The GDPR defines data protection[14] as "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

It is evident by comparing the DPD and GDPR definitions of personal data, then the latest definition is wider and includes more elements than the Directive it replaced, such as: "identification number, location data, an online identifier and genetic identity".

On the other hand, it should be brought up that the LOPDP of Ecuador defines personal data as: "Data that identifies or makes a person identifiable, directly or indirectly, in the present or future. Innocuous data, metadata or data fragments that identify or make a human being identifiable, are part of this concept."[15]

Unlike the GDPR definition, the LOPDP does not specify the elements that can make a person identifiable as their name, ID number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

[12] Opinion No. 4/2007 on the concept of personal data - WP 136 (20.06.2007)
[13] Millard, C., & Church, P., (2007a) 'Tissue Sample and Graffiti: Personal Data and the Article 29 Working Party' Computers & Law 2007, vol.18(3), pp. 27-29.
[14] General Data Protection Regulation (EU) 2016/679 Article 4
[15] LOPDP Articulo 5.

1.1 Data protection background in Europe

Regulating privacy and personal data in the EU started with the Universal Declaration of Human Rights of the United Nations (UN) in 1948, which is considered to host the earlier meaningful conversations about this topic.[16] This meant the recognition of the human right to privacy and its protection against arbitrary interference or attacks, according to Article 12 of the abovementioned UN Declaration.[17]

At across region and also European level, we can refer to the European Convention for the Protection of Human Rights (ECHR), signed in Rome in 1950 but effective since 1953 issued by the Council of Europe[18] as a milestone in the development and construction of data protection rights. The Article 8 of this text ratifies the right to respect for individuals and families privacy and establishes a right to privacy all over Europe. Its main objective is to ensure the balance of powers over the democratic participation in the processes of information and communication through the discipline of the systems of the obtainment, gathering and transmission of such data.[19]

Moreover, the right to the protection of information can be found also in the European Convention on Human Rights in its Article 10 guarantees the Freedom of Expression, explaining that this includes in its point 2 disposes that "…for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence…" The protection of reputation would be related to the right to privacy and on the other hand, to prevent disclosure of information received in confidence can be understood as giving our data for a fair processing or a specific purpose and being informed about it. The words "received in confidence" may tell us that it was also given in confidence, with consent over the transfer of such information.

Scholars like Robertson sustain that despite this Convention was far to be perfect, it meant a significant progress and advance on the Universal Declaration of Human Rights (UDHR) of

[16] Cate, Fred H. (1995) The EU Data Protection Directive, Information Privacy, and the Public Interest. Iowa Law Review 80(3), 431-444.
[17] Universal Declaration of Human Rights Art. 12. https://www.un.org/en/universal-declaration-human-rights/
[18] Council of Europe: an intergovernmental organization composed by more than forty States, aiming to promote democracy and human rights in Europe.
[19] Perez Luño, Antonio E. (1989) Los derechos humanos en la sociedad tecnológica. CEC, p. 138-139

the UN.[20] According to his analysis, the UDHR was a mere expression of intentions, when the ECHR disposed of explicit legal commitments adopted by fifteen European countries. For the purpose of this work, the most relevant innovative additions of the ECHR was the granting to individuals whose rights are denied of direct access to an international organ capable of protecting them, and also the creation of a binding jurisdiction among the subscripted countries, that expectantly would help to harmonize regulations over individuals rights in Europe.[21]

In the sixties, with new technologies arising and developing rapidly, the concerns for building an adequate legal and practical mechanism of protection of personal data and the right to privacy increased. The consequences of this fast development and the need of a proper legal framework were evident.[22] By the end of the decade the Council of Europe initiated analysis on personal privacy regulations among the Member States. As a consequence, in 1074 there were already resolutions providing short guidance of personal data protection for the banks operating in the Member States.[23]

The Council of Europe issued in 1981 in the city of Strasbourg the Convention for the protection of individuals with regard to automatic processing of personal data (CPPD), a treaty that in front of a rising cross border data flow, plans to protect individual's privacy and personal data, that comprehended several -but yet basic- data protection principles[24]. It was expected that this Convention harmonizes the regulations over the protection of personal data and privacy among the Member States, covering also the cross-border transfer of such data. The CPPD was a prototype of the integration of European regulations in regard to data protection and the transfer of such data, but still enabled the free movement of it.[25] This international treaty, according to the Council of Europe Portal[26] is the first binding

[20] Robertson, A. H. "The European Convention for the Protection of Human Rights." British Year Book of International Law, 27, 1950, p. 149-158.
[21] Ibid, p. 160-163
[22] Pearce, Graham and Platten, Nicholas (1998) Achieving Personal Data Protection in the European Union Journal of Common Market Studies Vol. 36, No. 4 pp. 529–47 p. 531
[23] Ibid.
[24] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28/01/1981
[25] Pearce, Graham and Platten, Nicholas (1998) Achieving Personal Data Protection in the European Union Journal of Common Market Studies Vol. 36, No. 4 pp. 529–47 p. 531
[26] The Council of Europe is a European Human Rights organization. Portal https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

international instrument made to protect the rights of the individuals and prevent the abuse in the collection and processing of personal data and that regulates the cross-border flow of such data.

Another event that can be considered a landmark in Europe development on the protection of human rights was the Oviedo Convention (OC) of 1997[27] as a result of the effort of the members of the Council of Europe. However, according to Roberto Andorno[28]the OC barely elaborates the right to respect for individuals and their families' private life, as the articles related to privacy do not contribute any instruction on the practical exercise of this right.[29] One of the main characteristics of the OC was the inclusion of the judicial protection by national courts, which by Article 23 of the mentioned Convention the States were required to "provide appropriate judicial protection to prevent or put a stop to an infringement of the rights and principles" of this same text.

Andorno also states that the explanatory reports from the OC point out that the above-mentioned European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data from 1981 covers the protections of individual's personal data sufficiently.[30] The OC, in regard to the topic of this work mainly focused on the right to be informed or not about their health condition.

Moving forward to more current times and to European regulations over the protection of personal data and the transfer of such data, after almost a decade since the CPPD was issued, the now existing European Commission[31] in 1990 started to discuss the need of a general framework for the processing of personal data inside and outside of Europe.

---

[27] Treaty No.164 Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine

[28] Member of the UNESCO International Bioethics Committee; Research Fellow at the Interdepartmental Center for Ethics in the Sciences (IZEW), University of Tübingen, Germany.

[29] Andorno, Roberto. (2005) The Oviedo Convention JIBL Vol 02. p. 139

[30] Ibid.

[31] The Commission consists of 17 members. The President is nominated by the Member States by common accord after consulting the European Parliament. As to the other persons, their nomination presupposes a prior consultation of the Member States with the Presidential nominee. The entire Commission is subject to a vote of approval by the European Parliament. EEC Treaty arts. 157-58, as amended by Maastricht Treaty, supra note 1, art. G, 31 I.LM. at 256. See also Bermann et al., supra note 1, at 55. https://ec.europa.eu/info/about-european-commission_en

Spiros Simitis[32] assures that the Commission's first intentions were to make the EU Member States to ratify the 1981 Convention of Strasbourg. However, he also mentions that the Commission knew that this treaty was not intended to replace national legislation of the Member States but only to act as a general guide[33] and it also lacked protection to the cross border flow of Europeans personal data, as per the free movements of goods across Europe, it was not blocked or obstructed.[34]

For almost twenty years, especially when the technology started to be an important tool to gather data- European countries have been concerned on regulating and harmonizing national legislations and international directives in relation to the transfer of personal data of their citizens among them.[35] They worked on agreements and regulations that aimed to guarantee an 'adequate' level of protection to personal data when transferring it from one country to another.[36]

Notwithstanding the progress and struggle on the protection of personal data and privacy rights and regulations, the discrepancies in between regulations of the Member States was evident and it seemed problematic to emulate the technology development and the amplification of the European community.[37]

In an attempt to update the protection of personal data and privacy in Europe, the Commission initiated a new framework that was supposed to work as a guidance to harmonize the internal regulations of the EU Member States. This contemporary scheme was proposed by the Commission in the 1990´s with a couple of clear objectives: a) Protect the fundamental rights and freedoms of individuals, and explicitly the ones related to their privacy regarding the processing of their personal data; b) the implementation of limits to the

[32] Professor of Law, Johann Wolfgang Goethe-Universitit, Frankfurt am Main.

[33] Simitis, Spiros (1995) From the Market to the Polis: The EU Directive on the Protection of Personal Data, 80 Iowa L. Rev. 445 p. 445-446.

[34] Free movement of goods, EEC Treaty art. 9, persons, id. art. 48, services, id. art. 59, and capital, id. art. 73b, as amended by Maastricht Treaty, supra note 1, art. G, 31 I.L.M. at 256. See aso Berman et al., supra note 1, at 317.

[35] Blume, P. 2015. EU adequacy decisions: the proposed new possibilities. International Data Privacy Law, Volume 5, Issue 1, p. 34.

[36] Cerda, A. 2011. The "Adequate Level of Protection" for International Personal Data Transfer from the European Union – Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, 36. Universidad Católica de Valparaíso. Valparaíso, Chile. pp. 327 - 328.

[37] Pearce, Graham and Platten, Nicholas (1998) Achieving Personal Data Protection in the European Union Journal of Common Market Studies Vol. 36, No. 4 pp. 529–47 p. 532

free movement of personal data over the EU and out of its borders.[38] These two main purposes that would be discussed in the next sub chapters.

The DPD was adopted by the Member States on 24 October 1995 after several discussions. This Directive established guidelines for the member states in order to adequate their national legislations in regard to the protection of personal data that was attempted in the past according to the progressive creation of the international instruments mentioned before.

The EU attempted to update the regulations over protection of personal data that the DPD was not covering any more regarding the transatlantic flow of European citizens' personal data -specifically to the United States of America- issuing at first the International Safe Harbor Privacy Principles in 1998 and almost twenty years after, the EU-US Privacy Shield.

Finally, we currently are subjects of the latest update and reinforcement of the European protection of personal data and privacy, that exists for the same reason that the last two mentioned instruments were created, based on the need of a sufficient legal framework to protect people rights to privacy and their personal data in times of light speed develop of new technologies and the increasing volumes of data flow across Europe and out of it, the Commission build the GDPR.

As per the above, there are regulations over data protection and the cross-border transfer of personal data in force even before the existence of the EU. The EU created Directives to provide a guideline on how to protect the cross-border data flow properly and therefore harmonize the protection of personal data among Member States. However, as a Directive is not mandatory it failed to force the Members to apply it, therefore, the regulatory frameworks for cross-border data flow available were still short.[39] As a consequence, the EU issued a Regulation, the GDPR, a guideline with more strict rules and a wider scope.[40]

These regulations and requirements look for a proper protection of personal data when it is transmitted among the countries which participate in the transmission of such data. These

[38] Ibid p. 537

[39] Svantesson, Jerker B. (2011) International Data Privacy Law Vol, 1 No. 3 pg. 180-195

[40] Buttarelli, Giovanni. (2016) The EU GDPR as a clarion call for a new global digital gold standard. International Data Privacy Law, 2016, Vol. 6, No. 2 p. 77-78

guidelines look forward to promote the respect to human rights, the market economy and democracy, setting patterns that aim to stimulate and encourage consistency between national and international laws in regard to the protection of data when it is processed or handled by public and private institutions.[41]

1.2 Data Protection Directive 95/46/EC of the European Parliament and of the Council

Due to the growing use of the internet, the transfer of data between countries is constantly increasing. In 1995, the European Union Member States adopted the Data Protection Directive,[42] which at that time was the only normative body which established patterns to be followed and also authorized application of the national laws of the countries involved in the processing and transmission of data, replacing the CPPD.[43]

With the implementation of the DPD, the European Union tried to harmonize the data protection regulations and its execution and practices among the Member States in order to contribute to the community integration in an attempt to the homologation of the regulations and even the judicial systems.[44]

The intention of this Directive is to harmonize as much as possible the regulations of data protection among the EU member states and it should not be considered as the sole Data Protection law of the Union. The Directives are principles or guidelines that the member states can or are suggested to follow and include them in their national regulations. Until the directive dispositions are not reflected in the member states national laws, the dispositions are not mandatory internally.[45] As a consequence we should see the Directive as a base in which each country can construct or reform their regulations over the relevant topic.

[41] Ibid.
[42] DPD OJ L281/31.
[43] Shakila Bu-Pasha (2017) Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law, 26:3, 213-228.
[44] Bainbridge, David I. (1997) Processing Personal Data and the Data Protection Directive. Processing Personal Data and the Data Protection Directive p.17
[45] Gilbert, Francoise (2007) A Bird's-Eye View of Data Protection in Europe, 24 GPSolo 32

The main objectives of this Directive as mentioned before were principally two. First to protect the fundamental rights and freedoms of individuals, and explicitly the ones related to their privacy regarding the processing of their personal data; and at second the implementation of limits to the free movement of personal data over the EU and out of its borders. Another of the purposes of this Directive was to safeguard EU citizen's personal data by establishing rules for the activities of data controllers in Europe that involve the transmission of such data to non EU countries and thus, the data collected and transmitted by EU controllers is then processed and gathered by the controllers of a non EU country.[46] It is assumed that the standards of protection are respected within the Member States.

Consequently, the activity of transferring personal data from an EU Member State to a third country implied the participation of public and private data controllers and processors from each county that is involved in the transaction.[47] Then, data is subjected to different regulations and guarantees in every port it reaches.[48] The DPD provisions have effect on the EU Member States data controllers and processors and also establish liabilities in regard of what is considered an infraction, but third countries controllers on the other side of the transmission are regulated by national laws which may not offer the same protection and/or guarantees than the mentioned European Directive.[49]

In this sense, the DPD establishes two different levels of protection for the movement of data. First, a level of 'equivalent' protection, which covers the transmission of data among EU Member States.[50] The second level is aimed at the transmissions between Member States and third countries, which ask for an 'adequate' level of protection of data.[51]

But what was the problem with the DPD in order for the European Commission to issue a new framework as a regulation? The main problem will be that as the title says, the DPD is

[46] Blasi, C. 2015. The limits of European data protection law in EU border control. Revista CIDOB d'Afers Internacionals. n.111, p. 128

[47] Shakila Bu-Pasha (2017) Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law, 26:3, 214.

[48] Tellez, Abel, La protección de datos en la Unión Europea, Madrid, Edisofer, 2002. p.45.

[49] Shakila Bu-Pasha (2017) Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law, 26:3, 214-215.

[50] Svantesson, B. 2011. The regulation of cross-border data flows. Published by Oxford University Press. Vol 1. No.3 p.p. 183

[51] Cerda, A. 2011. The "Adequate Level of Protection" for International Personal Data Transfer from the European Union – Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, 37.

a Directive, meaning that is not mandatory and is not the regulation of every European Member State.

EU Directives are no more than principles and suggestion guidelines which the countries should implement in their national laws, which they were failing to do, as it is not a mandatory European disposition. Another issue with the DPD was that as the principles sat here are not mandatory but a base, each country added their own restrictions and/or permissions that were not 100% aligned with the Directive, causing a difference among EU Member States National regulations over data protection.

Moreover, countries like Germany and Finland already had regulations over data protection before the 1995 Directive, which they did not modify or adapted to the DPD. The objective of this Directive of harmonizing personal data protection regulations was failing or better to say, they failed. The list of non EU countries that are considered to have an 'adequate' level of data protection are limited, and even more in regard to South American countries. Currently, the European Commission, under the DPD, has only recognized Argentina and Uruguay as the only two countries in the South of America which provide adequate' data protection.[52]

However, the GDPR which is replacing the DPD will be enforceable from May 25, 2018. This European legal instrument aims to harmonize as much as possible the rules over data protection within the European Union Member States and also non-EU countries with the force of a Regulation instead of with the mere guidance of a Directive.[53] It looks forward to improving data subjects' protection and to clarify the rules, establishing direct instructions to follow that must be complied in order to be considered to have an adequate level of data protection.[54]

The replacement of frameworks represented mainly symbolic and legal consequences. Symbolically it meant that the EU has tacitly recognized that the DPD was not strong enough to unify or harmonize Europe data protection Member States national regulations and,

[52] 2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina

[53] Tikkinen-Piri, C. 2018 EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer law & security review No. 34. University of Oulu, Finland. P.p. 135.

[54] Ibid.

legally, the upgrade of hierarchy of the framework from a mere guideline to a binging regulation. [55]

In order to improve the level of protection of personal data, the European Union has issued the GDPR, considered as an influential legal instrument with international effect and also acceptance.[56] Regarding the transfer of personal data to non EU countries, the GDPR has retained the requirements to be a county considered to have an 'adequate' level of protection. The new Regulation is considered as a landmark in the development and evolution of European data protection and privacy laws.[57] It is a legal instrument that guarantees data protection and privacy as they are considered fundamental rights.[58]

1.3. Background of the adequacy decisions in the European Union

The considerations of generic guidelines to protect personal data when transmitted abroad in virtue of commercial and intergovernmental activities can be appreciated in the Organization for Economic Cooperation and Development (OECD) from 1980. This organization member states and the United States adopted a guide of eight rules to harmonize the protection of personal data among the members of the OECD.[59] However, these guidelines were not legally binding, therefore the country's legislations did not necessarily need to adopt them.

As the Regulation relevant for this work is the GDPR, we will try to define what an adequate level in terms of the article 45 of this norm is. It establishes that an adequate level "where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection." Authors like Determann define this process as the Commission

[55] Hornung, Gerrit (2012) A general data protection regulation for europe? light and shade in the commission's draft of 25. SCRIPTed p. 65

[56] Shakila Bu-Pasha (2017) Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law, 26:3, 214-215.

[57] Goddard, M. 2017. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research Vol. 59 Issue 6. P.p. 703.

[58] Alexy, Rober. (2007). "Los derechos fundamentales en el Estado constitucional democrático". Centro de Estudios Constitucionales. p. 135

[59] Nikhil S. Palekar, (2008) Privacy Protection: When Is Adequate Actually Adequate, 18 Duke J. Comp. & Int'l L. p. 551

issuing decisions "on the adequacy of the protection of personal data in third countries."[60] An adequacy decision can be defined as an award of the Commission to a non-Member State that certifies it offers a sufficient legal framework with adequate protection for an individual's personal information and their rights and freedoms over it.

The internet's first documented appearances in history can be considered since 1962 when the Massachusetts Institute of Technology worked with a concept of a Galactic Network, this was followed by many other developments in network communication during the 1970 and 1980. With the advance of the technology and the exponential growth of the use of the Internet, the transfer of personal data abroad became a daily routine that has just increased its volumes. It is a fact that the cross-border data flow has been happening a long time before the internet or any communication network system, however it can be said that the internet has contributed to fast and borderless information transportation.

Subsequently after the resolution of these eight principles, and as a response to the fast development of technology and the increasing volumes of data flows, the Council of Europe issued the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[61] Despite both before mentioned guides attempted to equalize data protection among different countries with certain success, they still were vulnerable as they were not of direct applicability, but a mere directive and also failed to balance privacy and economic or commercial activity.[62]

A practical example of an historical appearance of cross border personal data protection and adequacy decisions, despite not being an EU Member State, is the Swedish and their Data Act of 1973 could be considered an example for European countries. The Article 11 of the Swedish Data Act established: "If there is reason to assume that personal data will be used for automatic data processing abroad, the data may be disclosed only after permission from the Data Inspection Board. Such permission may be given only if it may be assumed that the disclosure of the data will not involve undue encroachment upon personal privacy."

[60] Determann, Lothar, Adequacy of Data Protection in the EU - General Data Protection Regulation as Global Benchmark for Privacy Laws? (January 17, 2017). Available at SSRN: https://ssrn.com/abstract=2902228

[61] George, Barbara (2001) et al., U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive, p. 744.

[62] Boyd, Virginia (2006) Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization, 24 BERKELEY J. INT'L L. p. 957

The inclusion of an official permission to process data abroad serves as an historical milestone regarding the validation of protection mechanisms offered by third countries. The Swedish apparently had reasons to believe that their citizen's personal information was going to be processed abroad, there is the possibility of already being aware of the consequences of the internet and the communication technologies or communication network development. The need for the approval of the Swedish Data Inspection Board for the process of Sweden citizens' personal data abroad gives us a reason to believe they had standards of protection over personal information. By "Such permission may be given only if …" we can interpret that the legislator attempts to prevent abroad and local data processors and or controllers from eluding Sweden's data protection regulations by taking their operations to third countries with lower data protection exigency or more permissive laws.[63]

Back in Europe and moving forward in time, the mentioned DPD aimed to set principles and standards for the protection of personal data among the member states and also disposed of rules for the Commission in order to determine adequacy level of protection.[64]

These adequacy rules aimed to avoid the processors going over the Directive regulations by processing or transmitting Europeans personal data in third countries with a less strict standard of protection.[65]

With the purpose of mitigating the impact of the restrictions to the overseas transfers of personal data provided by the previously mentioned article of the DPD, the EC and the United States agreed on adopting the Safe Harbor in the 2000, issuing the Decision 2000/520[66] in order to guarantee the uninterrupted flow of data between the US and the EU by assuming an adequacy level of protection of both parties.

This last agreement sets parameters to provide a satisfying protection to privacy and personal data transferred overseas. By remaining within the demands of the Safe Harbor agreement,

[63] Bygrave, Lee A. (2002) Data Protection Law—Approaching its rationale, logic and limits. Kluwer International) pg. 79-80.
[64] Directive 95/46, 1995 O.J. (L 281) 31.
[65] Nikhil S. Palekar, (2008) Privacy Protection: When Is Adequate Actually Adequate, 18 Duke J. Comp. & Int'l L. p. 552
[66] Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC).

the US and EU business should be in compliance with the European data protection and privacy principles.[67]

The ruling of the European Court of Justice in their judgment of 2015 — Case C-362/14 Maximillian Schrems vs. Data Protection Commissioner[68] was the breakpoint for the start of an update on the protection of Europeans personal data abroad. Mr. Schrems is an Austrian citizen who has been a user of the social network Facebook since 2008. Schrems submitted a complaint regarding the transfer of his data to the USA by the mentioned social network against its subsidiary branch in Ireland sustaining that his consent to Facebook's data use policy did not cover several data use processes carried by the social network. The previous was a consequence of Edward Snowden leak and disclosure of a surveillance program carried by the NSA, capable of tracking Internet users, monitoring and analyzing big data among other unlawful applications of the data.[69]

The Court declared the Safe Harbor agreement invalid as it did not provide enough guarantees based on the EU standards. As a consequence, US companies would need to fulfill the lack of adequate data protection with binding corporate rules, and also, restrict the access of the USA authorities to European citizen's data.[70] The Court decided that the flow of Europeans personal data to non-member states should be treated with an equal level of protection as within the EU. The decision of the Court and the conversations between the US Department of Commerce and the EC led to the EU-US. Privacy Shield, in which both authorities have reached agreements and have amended disposition in regard to the processing of Europeans data by American companies.[71] However, the US was aware of this agreement being compliant with the DPD, but not with the GDPR that was already in discussions.

---

[67] Ibid. p. 556

[68] Case C-362/14 Maximillian Schrems vs. Data Protection Commissioner https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN

[69] Class Action Against Facebook Ireland, EUR. VERSUS FACEBOOK (Dec. 1, 2015), http://europe-v-facebook.org/EN/Complaints/Class_Action/classaction.html. quoted in Beata A. Safari, (2017) Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, 47 Seton Hall L. Rev. 809

[70] CJEU: First Reaction to AG's Opinion on NSA "PRISM" Scandal Facebook's EU-US

[71] Press Release, European Commission, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-releaseIP-16-216_en.htm.

The EU by implementing this new regulation looks forward to having a standard set of rules and a higher level of protection for personal data and privacy abroad. IT can be said that non-European countries are reforming their legislatures to be in line with the GDPR and therefore be considered to offer an adequate level of protection in benefit of the commercial and political relations with the EU.[72] The GDPR among other purposes intends to harmonize cross border data protection regulations within member states and also invites non EU countries to follow these rules, looking forward to using it as a solution to the challenges presented to the cross border data flow. It also differentiates from the DPD adding rules and looking stricter against the protection of data abroad.[73]

Being awarded with an adequacy decision from the EC would allow the transfer of personal data from EU Member States to non-member states, like Ecuador, without the need of additional guarantees or security measures from each side, meaning the transfer of personal information between the EU and the third country with the adequate level of protection would be treated as it was inside the EU.

1.4 European Commission Adequacy Decisions under Directive 95/46/EC

The European Commission has so far recognized Andorra, Argentina, Canadian commercial organizations, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and the United States of America as non EEA (European Economic Area) countries that provide an adequate level of protection of personal data under the expired DPD.

1.4.1 Adequacy Decision of Argentina

As mentioned previously in this work, the European Commission has awarded several non EU Member States with the calcification of being a country that offers an adequate level of personal data protection. The EC made the decision over Argentina adequate level of

[72] Wagner, Julian (2018) The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? International Data Privacy Law, Vol. 8, No. 4 p. 319
[73] Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya A.P. Ramanathan (2017) Cross border data transfer: Complexity of adequate protection and its exceptions. Computer law & security review p. 3

protection on June 30, 2003.[74]

In 2002, the Working Party[75] issued a favorable opinion for Argentina. This opinion admitted that they found the national legislation guarantees an adequate level of protection based on the DPD parameters, however, it also encourages the authorities to take action in order to update and solve issues that the current legal framework over data protection might contain.

Moreover, it invites the local government to guarantee the application of the law by creating or giving autonomy to control bodies in the rural areas of the country that for the moment, can be solved by recurring to the constitutional norm.[76]

The Personal Data Protection Law in Argentina derives from the Constitutional right of *Habeas Data*, which is the right to access, modify or suppress personal data. This is a guarantee that the Ecuadorian Constitution also provides.[77]

After discussions and amendments to the Argentine Data Protection Bill, in 2000 it was finally adopted as Law creating a regulatory institution and providing a legal framework for the application or execution of the *Habeas Data* Constitutional right, also disposing rights and obligations for data subjects and processors.[78]

Considering the provisions and principles that motivated the Argentinian Personal Data Protection Law (APDPL), they are quite similar to the ones described in the DPD. However, there are substantial differences that were not a big barrier for the Commission in order to decide over this country adequacy level of protection.

One of the differences we can find between APDPL and the DPD is in the definition of personal data. As mentioned before, Europeans care so much for their privacy and data protection that the concept of what is considered personal data is wider than in any other of the compared legislations, even before GDPR which has an even wider scope.

---

[74] Ibid.

[75] Directive 95/46/EC Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data

[76] Opinion 4/2002 on the level of protection of personal data in Argentina

[77] Gakh, Maxim. (2005) Argentina´s Protection of Personal Data: Initiation and Response. p. 782

[78] Ibid p. 782-783

Another difference is the meaning given to the "processing" of data. The APDPL comprehends two categories for this, the data treatment and the data dissociation, both related to the operations made over this data. On the other hand, the DPD considers these two categories into one, the data processing.

The Argentinian Law contemplates three types of individuals: data owner; data user and; person responsible for the data. The DPD defines these individuals as data subject and; data controller. Despite being just a wording difference, the DPD puts the data owner and data user as one under the data subject definition.

The Directive, as per its nature, unlike the APDPL is not mandatory, making the law purpose more executable and reachable for the individuals. The Argentinian Law provides precise rights and obligations to its subjects in order to protect personal information stored in private and/or public databases and with the specific purpose of making the right to *Habeas Data* accessible, meaning that the individuals now have a mechanism to access, modify and delete their personal information.

Regarding differences on rights and obligations provided by these two legal frameworks, it is important to mention again that in practice and by its nature, a law has a higher level of hierarchy over the Directive.

The Argentinian Data Protection Law and the DPD have similar structure principles and considerations that focus on the fairness of the data processing and the right of the data subjects to give consent, have access to their information and define obligations for data processors.

The APDPL like the DPD requires that the data collected to be processed has a purpose, a fair objective which is appropriate and proportional to the requirement of such data, avoiding the excessive and unnecessary collection of personal data, meaning that the processing of personal data should have a limited or specific purpose. Moreover, both the Directive and the APDPL contemplate the right of the data subjects to access and modify their data and the option to be erased when the specific purpose has been fulfilled.

The Argentinian Data Protection Law, as mentioned before, also provides the data subject the right to give their consent in order for their personal data to be processed.[79] Nevertheless, the Law contemplates exceptions to this rule when there is no need for consent. Such exceptions are applicable when the personal data is public; it is needed for the performance of a national duty or; when such data comes out of a contractual relation.

An interesting disposition in Argentine Law is that the data subject has also the right to be notified when a third party has requested their data. This notification has to include: the purpose, the level of the obligation to provide it (if it is mandatory or voluntary) and the consequences of providing, refusing or giving incomplete or inaccurate data.[80] According to the APDPL, there are four main rights of personal data that comply and are aligned with the DPD requirements as it provides the right to be informed, access their information, rectification and erasure. [81]

On the other hand, the APDPL also disposes obligations for data controllers and processors. The data processing cannot be delegated by the processor in order to keep its confidentiality and they are obliged to implement measures that ensure the security of the data. Moreover the ADPDL creates a governmental authority with the purpose of ensuring the protection of data and the law compliance by the processors, which is the regulatory body in Argentina.

The EC determined that the Argentinian legislation disposes of the fundamental principles regarding personal data protection, such as the purpose limitation or fair purpose, proportionality, transparency and security and on the other hand the data subject rights to be informed, to access their information, to rectification, apposition and data erasure. Argentina also counted with mechanisms and processes that ensured the access and the appliance of these rights and principles prescribed by the law according to the EC.

The Commission considers Argentina to have general and specific standard rules with binding legal effect on the protection of personal data.[82] It points out the legal framework mentioned previously composed of the Constitution, the APDPL and its ruling of application.

[79] Law for the Protection of Personal Data, Argentina, supra note 33. 5
[80] Ibid, supra note 33. 6
[81] Ibid, supra note 33. 16
[82] Ibid (5)

It remarks the presence of the resource of *Habeas Data* as a fundamental right included in the Argentina Constitution. Additionally it takes into consideration the existence of a law that executes the dispositions of the Constitution.[83] Moreover, the EC acknowledges the protection of personal data recorded or stored in technical or physical, public or private means. It contains principles and obligations for data controllers and processors and appoints the existence of other data protection related dispositions spread in other regulations.[84]

The Commission explicitly mentions in its Decision that "Argentine Law covers all the basic principles necessary for an adequate level of protection for natural persons, even if exceptions and limitations are also provided in order to safeguard important public interests." An important element that the EC includes in the Decision is that Argentina provides quick administrative and judicial solutions and a control authority with autonomy.[85] It should be brought up that the EC also takes into account the conversations with the Argentinian government and their assurance of the compliance and application of the law.[86] Adding a quote of trust and negotiation to the process of making an adequacy decision.

To summarize, it can be said that the main considerations of the EC in regard to the Argentine legal framework regarding data protection were to have a satisfactory level of the law, an authority to protect privacy and personal data rights and provide adequate mechanisms to claim them.[87]

1.5 General Data Protection Regulation

The GDPR contains considerably more rules and guarantees for data subjects and amplifies the roles and responsibilities of data processors. Furthermore, as it is a binging regulation, it contains fines for breaches or violations to individual's rights or omission of processors duties.[88] In May 2018 the GDPR came into force after two years of discussions. During this

[83] Ibid. (7) (8)
[84] Ibid (10) (11)
[85] Ibid (13) (14)
[86] Ibid (15)
[87] Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina
[88] Hornung, Gerrit (2012) A General Data Protection Regulation for Europe? Light and shade in the Commission's draft of 25. SCRIPTed. p. 64

time EU Member States had enough time to make the necessary amendments in order to be compliant with the new regulation.

1.5.1 GDPR effect on third countries

There is a dark history of events that started, consummated and perpetuated with personal data misuse across the world, therefore, data protection is very important for the EU and its citizens. The importance goes to the extent that it crosses jurisdictions if needed, coercing its mandate outside borders when Europeans data has crossed them for whatever reason.[89]

The GDPR in its article 3 it defines its territorial scope, making the Regulation[90] have jurisdiction over processors not only within the EU but also in countries out of it. As a consequence, it establishes requirements that non-member states legislations over data protection must include. A clear example is the United States, where many Information and Communication Technology companies are domiciled, need to comply with the local regulation and also with the GDPR if they process or gather Europeans personal data.[91]

Generally speaking, the above mentioned regulation covers relevant changes regarding the data protection rights of European citizens. As stated before, one of the main points that has been reinforced is the transmission of data to third countries.[92] Additionally, the GDPR aims to harmonize data protection regulations among the EU Member States and third countries that are part of the process of the transmission of data. This harmonization looks forward to solving the problems arising from the differences of every country's regulations over data protection.[93]

One of the most relevant aspects of the GDPR is that it keeps demanding a third countries adequacy level of protection to EU personal data. This adequacy is measured by a test that

[89] Safari, Beata A. (2017) Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, 47 Seton Hall L. Rev. 821
[90] GDPR
[91] Safe Harbor Certification, PRIVACYTRUST (2016), http://www.privacytrust.com/guidance/safe harbor.html.
[92] Pardis, Tehrani, Johan, Bin Hj, Dhiviya A.P. Ramanathan, 2017. Cross border data transfer: Complexity of adequate protection and its exceptions, Computer Law & Security Review: The International Journal of Technology Law and Practice . doi: 10.1016/j. p.p. 3
[93] Ibid.

determines which country can be awarded or authorized as a safe port to European data.[94] The 'approval' of this test will mean that the third country is considered to provide adequate protection. As per the example of Japan exposed in the next subchapters, the GDPR does not demand a full and complete match of the non EEA countries legislation over data protection with the legal dispositions of these regulations, but it considers adequate when the fundamental principles and rights are aligned with it.

1.5.2 Cross-Border Personal Data Transfer under General Data Protection Regulation

In comparison with the DPD, the GDPR sets new requirements in regard to cross border data flow. For instance, it includes a code of conduct and a certification mechanism, with the purpose of improving the protection of Europeans personal data abroad.[95] The code of conduct aims to be a support for the controllers and processors in order to demonstrate their capability to provide sufficient appropriate safeguards. On the one hand the certifications are a guarantee stamp of being complying with security standards.[96]

The uninterrupted flow of data within the EU is considered to be elementary in the development of the Single Market, therefore the GDPR seeks to balance privacy and data protection with the business activities and the commerce among the member states by implementing common rules to the processing of personal data.[97]

Cross border processing in the GDPR is limited to two scenarios: "1) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or 2) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State."[98] For purposes of this work we will discuss the cross border

[94] Ibid.
[95] GDPR Art. 31 and 48
[96] Meyers, Anna (2016) 'Top 10 operational impacts of the GDPR: Part 4 – Cross-border data transfers' <https://iapp.org/ news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border -data-transfers/
[97] Wagner, Julian (2018) The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? International Data Privacy Law, Vol. 8, No. 4 p. 320
[98] GDPR Article 4. (23)

data transfer restrictions for recipients out of the EEA.

According to the article 45 of the GDPR, the EC is the authority responsible for determining which non EU countries offer an adequate level of protection considering their national legislation and international agreements which they have become part of among other requirements and conditions related to these two normative bodies.[99]

As a consequence, the effect caused by the GDPR over the transmission of personal data goes beyond the boundaries of the EU Member States. The regulation influences directly into third counties and non-European private and public institutions and bodies.[100] Its scope is practically worldwide.[101] This Data Protection legislation is restrictive for the transfer of personal data to non EEA countries with the exception that those countries have been considered by the EC to offer an adequate level of protection over personal data. These restrictions apply to all data transfers despite their size or how often in time is processed.

In relation to the transfer of data to non-Member States, the GDPR as the DPD contains a list of dispositions that allow certain transfers of personal data based on an adequacy decision or by the provision of appropriate safeguards, just like the Directive. A restricted transfer can be defined as any transfer of Europeans personal data to a country in which the GDPR is not applicable, in this case, out of the EEA. A restricted transfer can be made, in accordance with the GDPR, to those non EEA countries awarded by the Commission with an adequacy decision; by providing the appropriate safeguards and the exceptions provided in the GDPR.[102]

If the country receiver of the personal data is among the ones considered by the Commission as offering an adequate level to data protection, the transfer of restricted data can be done without further requirements or authorizations from the administration. This method of cross border personal data transmission will be analyzed in detail in the following subchapters, as

[99] Blume, P. 2015. EU adequacy decisions: the proposed new possibilities. International Data Privacy Law, Volume 5, Issue 1, p. 36

[100] Kuner, C. 2017. The GDPR as a chance to break down borders. International Data Privacy Law, 2017, Vol. 7, No. 4. p. 231

[101]

[102] Hornung, Gerrit. (2012) A General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft of 25 January 2012, 9 Scripted 64. Pg. 70-72

it is the main matter of this work.

When a country is not awarded with an adequacy decision the transfer of personal data from an EEA country to that non-awarded third country, the regulation imposes restrictions to the transfer of such data but also includes exceptions and alternatives to allow the transfer of personal information. If there is no adequacy decision, the data processor needs to verify that the country destiny of the data provides the appropriate guarantees that the GDPR establishes.

In accordance with Article 46 of the GDPR, the transfers subject to appropriate safeguards can be considered "on condition that enforceable data subject rights and effective legal remedies for data subjects are available." Meaning that even if these safeguards are available, if there are no appropriate legal remedies for data subjects, the restriction applies.

The same article includes 6 appropriate safeguards that may be provided by:

(a) A legally binding and enforceable instrument between public authorities or bodies;
(b) Binding corporate rules (BCR) in accordance with Article 47;

Article 47 provisions regarding binding corporate rules are in accordance with the consistency mechanism set out in Article 63, requiring the following 3 aspects:

- Legally binding, applicable and enforced by every member part of a joint economic activity.
- Existence of enforceable rights regarding the processing of personal data; and
- Fulfil all the requirements established in paragraph 2 of this same article, which includes 14 requirements that the binding corporate rules shall specify.

(c) Standard data protection clauses adopted by the Commission (examination procedure referred to in Article 93(2));
(d) Standard data protection clauses adopted by a supervisory authority and approved by the Commission;
(e) An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

As it is for most of the rules there is an exception. In this case the GDPR provides 8 exceptions for restricted transfers.

The first exception relies on the consent of the data subject for their personal data to be transferred and processed abroad. Another exception would be to have a contract with the individual and the transfer of their data is necessary for the fulfillment of the contract or steps necessary to create or execute the contract.

Moreover, if there is a contract with an individual in benefit of a third person who is the owner of the data being processed or transferred and it is necessary to get to or execute the contract. The fourth exception would be a restricted transfer for public interest.

The fifth exception is the case when there is the necessity of making a restricted transfer for the purposes of having, making or defending a legal process. Restricted transfers with the purpose of protecting the vital interest of an individual who is physically or legally incapable of giving consent are also excluded from the rule.

Administrative data transfers such as the transfers made form public registries are excluded. And the last exception to the rule is when making a one-time restricted transfer within your legitimate interest.

Two types of appropriate safeguards are determined, as follows: the safeguards that do not require any specific authorization from a supervisory authority and the safeguards that can be used based on an authorization.

The appropriate safeguards that do not require authorization are standard data protection clauses adopted by the EC, standard data protection clauses adopted by a supervisory authority, BCRs for multinational groups of companies such as an approved code of conduct

and an approved certification mechanism.[103] However, they are required to be used together with binding and enforceable commitments of the controller or the processor in the third country to apply the appropriate safeguards.

An authorization from the supervisory authority is required for a transfer(s) if it is based on contractual clauses between the controller or the processor and the data recipient or provisions of administrative arrangements between public authorities or bodies.

1.5.3 Adequacy Decisions under General Data Protection Regulation

The Commission is the authority that is in charge of performing the adequacy and authorization procedures to determine whether a third country has or not appropriate level of data protection based on the faculty that the article 43 of the GDPR establishes in regard to the requirements prescribed in article 45 of the same legal instrument.[104] This authorization given by the Commission allows the free flow of data between the EU Member States and the third country considered as having an adequate level of protection for the European data with no additional safeguards. [105]

According to GDPR, an adequacy decision is one of the methods to ensure the protection of Europeans personal data abroad. The adequate level of protection should be determined by considering the third country legal framework and its protections towards the access of the administration or governmental bodies to individuals' personal data.

Third countries that are willing to offer sufficient data protection guarantees should take into consideration using the GDPR as an example.[106] Also, as a token of an intention to harmonize regulations of activities that can easily cross borders, such as transferring data.[107]

All democratic countries shall ensure improvement and reinforcement of all the fundamental

[103] GDPR Art 40, 42

[104] Gakh, Maxim. (2005) Argentina´s Protection of Personal Data: Initiation and Response. p. 794-795

[105] Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya A.P. Ramanathan, 2017. Cross border data transfer: Complexity of adequate protection and its exceptions, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.

[106] Tikkinen-Piri, C. 2018 EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer law & security review No. 34. University of Oulu, Finland. P.p. 145

[107] Kuner, C. 2017. The GDPR as a chance to break down borders. International Data Privacy Law, 2017, Vol. 7, No. 4. P.p. 231

rights of a democratic society.[108] By adopting or/and adapting the GDPR to their national legislations, the third countries can be benefited in two ways. First, for their own legal security, it is very important for the economic development of a country. Second, to comply with the GDPR and offer an adequate protection of data, which will also help to ensure legal security. [109]

Nevertheless, the adequacy is not related only to regulations that ensure data protection. The GDPR also looks forward to giving the qualification of a level of adequate protection to those countries that are not in a political crisis, which explains why only two of all South American countries are recognized by the Commission.

Considering this, and the complexity of the GDPR, the scenario is not favorable to the other countries in the South of the American Continent. The reforms to the national legislations needed to comply with the requirements imposed by the GDPR are the main challenge. The standards of governance and justice that the GDPR requires can be a bigger barrier.[110]

In this sense, for a South American country to be up to the requirements of the GDPR can take years of discussions and a significant monetary investment. Nevertheless, it should be possible using and following the discussions and evolution of the European Data Protection Regulation.[111] The GDPR actually prescribes that the EU shall be the protagonist issuing initiatives to encourage and help third countries to improve their data protection laws. Especially to those countries with limited economic and institutional resources.[112]

The GDPR, in its article 45: 2) sets the components that the Commission takes into consideration to evaluate the adequacy level of protection. Only those countries that fulfill the requirements are considered by the EU to have an adequate level of data protection.[113]

---

[108] Alexey, R. (2014) Constitutional Rights and Proportionality. Journal for constitutional theory and philosophy of law. p.p 142.

[109] Tikkinen-Piri, C. 2018 EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer law & security review No. 34. University of Oulu, Finland. P.p. 144

[110] Svantesson, B. 2011. The regulation of cross-border data flows. Published by Oxford University Press. Vol 1. No.3 p.p. 184

[111] Kuner, C. 2017. The GDPR as a chance to break down borders. International Data Privacy Law, 2017, Vol. 7, No. 4. P.p. 232

[112] GDPR Art. 50.

[113] Blume, P. 2015. EU adequacy decisions: the proposed new possibilities. International Data Privacy Law, Volume 5, Issue 1, p. 35

The elements to take into account are the rule of law; independent supervisory authority and; International commitments entered into by the third country or the international organization.[114]

If the commission has not adopted an adequacy decision, and the specific transfer of data does not fall into the exceptions mentioned before, the GDPR requires from the controller or the processor appropriate safeguards, in a legally binding instrument, for transfers to third countries or international organizations. The adoption of an adequacy decision from the EC involves[115]:

- a proposal from the EC
- an opinion of the European Data Protection Board[116]
- an approval from representatives of EU countries
- the adoption of the decision by the EC

1.5.3.1 Japan Adequacy Decision

The EC issued an adequacy decision for Japan in 2018. This nation is so far the only country awarded with a decision of personal data protection adequacy under the GDPR ruling and also called by the EU as the largest area of safe data flow across the globe.[117] This means that Japan when receiving personal data coming from the EEA for commercial purposes it is processed with an adequate level of protection.

After an age of not so protective rights for privacy and personal data, in 2015 Japan started a transformation of their legislature in regard to these two rights. Several changes were made in the Japanese Act on the Protection of Personal Information since then. The objective of the amendments was to make the Japanese legislature over data protection and privacy as similar as possible to the European rule.[118]

---

[114] GDPR Art. 45 2.

[115] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[116] European data protection board Article 68 GDPR

[117] European Commission Press Release IP/10/421, European Commission Adopts Adequacy Decision on Japan, Creating the World´s Largest Area of Safe Data Flows (Jan 23, 2019)

[118] Schwartz, Paul M. (2019) Global Data Privacy: The EU Way. New York University Law Review. Vol. 94:771 pg.787-788

The scope of personal data in the Japanese Law is smaller than the one in the European GDPR. The Japanese Act sets aside personal information that is not in a personal information database. As a personal opinion, we assume all of our names and dates of birth are registered somewhere by law as soon as we are born, the problem is that personal information is not limited to our name and birthday. Apparently, Japan leaves a breach that the Commission considered adequate somehow.

Another limitation to personal data scope is that the Japanese Act excludes the personal data that has a chance of violating other individuals' rights and interests. Moreover, the pecuniary penalties imposed by Japan over violations to the data protection law are softer and permissive. There is also a big room for mass surveillance from the Japan government bodies, which have permission to interfere with citizens' communications[119].

On the other hand, as Japan intended to align as much as possible to the GDPR and the European culture over data protection, despite of the mentioned significant gaps attributed mostly to cultural differences,[120] there are clear similarities between both legal blueprints for data protection and privacy rights.

The main similarities rely on the principles of the GDPR, the safeguards required for international data transfers and access to justice in regard to data protection violations. One of the big implementations of Japan is the creation of a governmental body which acts as authority towards data protection matters. The Personal Information Protection Commission is an independent institution that enforces the authority to ensure data protection and privacy rights of individuals are enforceable.

Japan added to their legal framework other safeguards for the data coming from the EU. This was one of the main components that led to the adequacy decision of the EC, together with governmental negotiations and promises related to the security of personal data and the access to it from Japan public servants being proportional and limited such as in Europe. At last, like Argentina, the EC considered Japan to have a complaint-handling structure that

[119] Greenleaf, Graham (2017) Questioning 'Adequacy' (Pt I) – Japan 150 Privacy Laws & Business International Report, 1, 6-11 UNSW Law Research Paper No. 18-1

[120] Yohko Orito and Kiyoshi Murata (2005) Privacy Protection in Japan: Cultural Influence on the Universal Value p.3-4

would investigate and solve Europeans complaints.[121] The EC concluded that the Japanese legal framework which included the law mentioned before, the supplementary measures of the Annex II of the Decision and also the assurances and promises from the government officials all together provide level of protection for personal data transferred from the EU, and that this protection is essentially equivalent to the GDPR previsions.[122]

As a conclusion, in order to determine an adequate level of protection, the EC considers elemental that the country offers at least the following three provisions: 1) Have a legal framework in regard the protection of personal data that covers as much as possible the provisions of the GDPR, including general and specific dispositions as mentioned in the relevant subchapter of this work; 2) the existence of an independent authority which is in charge of acknowledging and resolving data subject claims in regard their personal data and the rights related to it, and; 3) the implementation and applicability of mechanisms that will allow the data subjects to claim their rights.

[121] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421 European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows (2019)
[122] Commission implementing Decision (EU) 2019/419 of 23 January 2019 4. L 76/31 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information

2. DATA PROTECTION FRAMEWORK IN ECUADOR

Ecuador lacks regulations and suffers a partial absence of data protection principles. Despite of the Constitution of the Republic of 2008[123] (the Constitution) gives the State the responsibility to guarantee the right to privacy and data protection. However, these voids left by the lack of a data protection law have attempted to fulfill in part by disperse dispositions in different national laws and international agreements.

Despite containing the right to privacy and personal data protection, the Constitution provides a mere instruction that needs to be followed by laws and rulings to ensure the respect to these rights. The protection granted by the Constitution is not enough as it is very broad and it does not define what is considered personal data.

Personal data definition per se can only be found in the Electronic Commerce, Electronic Signatures and Data Messages Law as "the data or information of a personal or intimate nature, which are a matter of protection under this law."

In the next few subchapters we will analyze the current and in force Ecuadorian legislation that in any form include dispositions for the protection of personal data in order to expose how it currently works in practice.

2.1. Background on Data Protection in Ecuador

Even after the independence from the Spanish Crown in 1809, the abuses to the indigenous and other cultural discrimination stayed in the society. Personal or sensitive information was used by the authorities in order to determine rights for different groups or ethnicities.[124] In the 1800 there was almost no respect for individual's constitutional rights or even human rights. The beginning of the foundation of the State in the independent country began in

[123] Political Constitution of the Republic of Ecuador 2008
[124] Caillavet Chantal. (2000) Etnias del Norte: Etnohistoria e historia de Ecuador

the1830, with the first Political Constitution.[125]

As a curious fact, the few rights recognized in the first constitution were divided for groups. There were rights attributed just based on the place of birth and rights accessible to citizens. Citizenship rights were exclusive for those individuals with the Ecuadorian nationality. However, in order to access these small amounts of rights there were some requirements to fulfill, for example, having land worth more than a certain amount, have a profession and know how to write and read.[126] Ecuador started to get into a path to a State of Rights with the beginning of the Liberal Revolution in 1895 to 1912, a process of economic, social and political transformation. However, here we can still clearly see a not fully vested State of Rights, as the Liberal leader Eloy Alfaro, was murdered and dragged around the streets of Quito by the populace on 28 of January in 1912.[127]

Moving forward most recent events, specifically to the adoption of rights related to personal data protection, the figure of *Habeas Data* was incorporated in the Constitution of 1996, two previous texts before the current Constitution of 2008. In the next subchapters we will compare the definition and scope of *Habeas Data* according to the 2008 Constitution considerations.

Ecuador is obliged by the Universal Declaration of Human Rights, and also by many other international treaties on human rights at an American continent and also cross continent level. Despite of all the international instruments and constitutional guarantees, the governments and congressman of the day during the past two hundred years of independence and development of a State of Rights have fail to create a regulation over the protection of personal data, making only spread dispositions among a few weak laws or rules with soft sanctions for data protection and privacy violations, and the lack of mechanism to ensure the protection of such rights.

As mentioned in the introduction to this work, in September 2019 Ecuador went through a public scandal involving more than seventeen million Ecuadorians personal information such

[125] Enrique Ayala Mora (1993) Resumen de Historia del Ecuador. Época Republicana Segundo Periodo Tercera edición actualizada Corporación Editora Nacional. Quito, 2008 Biblioteca General de Cultura.
[126] Political Constitution of the State of Ecuador 1830, Art. 10-11-12.
[127] Concha, Jorge. (1942). Eloy Alfaro: su vida y su obra. Talleres Gráficos de Educación. Quito.

as civil data and financial information. The BBC revealed that almost every single Ecuadorian personal data was leaked and totally exposed on the internet to public access in an unsecured cloud. The breach was pointed out by the security company vpnMentor[128].

The BBC in its report about this data leak quoted Catalin Cimpanu, a reporter for the ZDNet, who expressed that this data is "as valuable as gold to criminal gangs", as with the data available it was easy to find the wealthiest citizens, their address, cars, banks and the most scary, their children personal information. The access to the data was interrupted by the Ecuadorian information security team.

The project for the Organic Law on the Protection of Personal data was submitted by the President Lenin Moreno on September 19, 2019, two or three weeks after the leak acknowledgment and three days after the BBC news. However, until the date of the finalization of this work, the Bill has not been approved.

2.2. Personal Data Protection in the Political Constitution of the Republic of Ecuador

The current Ecuadorian Constitution of 2008 provides a wide list of rights and guarantees including the right to privacy, personal data protection and the resource of *Habeas Data*. Article 40 of the *Magna Carta* refers to human mobility and the right of the people to migrate. This article establishes that the State, through its administration bodies, will develop actions for the rights of the Ecuadorians abroad despite their migratory status. One of the actions to take is to maintain the confidentiality of the personal data stored in files in the Ecuadorian institutions abroad.

As a Constitutional State of Rights, the dispositions prescribed in the Constitution are at the top of the legislation hierarchy, over all the rest of laws including International Agreements and Organic Laws and also over the government entities and Legislative and Judicial powers

[128] Data on almost every Ecuadorian citizen leaked. September 16, 2019. https://www.bbc.com/news/technology-49715478

of the State.[129] Following a sequential order, the next constitutional right related to the protection of privacy and personal data is established in the Article 66 which comprehends the liberty rights, the State recognizes guarantees the right to keep our convictions privately, for ourselves, and no one can be forced to declare or disclose them.[130]

In the same Article the constitution recognizes the right to personal data protection, including the access, protection and disposition of such data. It disposes that an individual consent is required for the gathering, store, process, distribution or diffusion of their personal data, except when it's mandatory by law.[131] Like in the Argentina and Europe legislations, there are exceptions determined by the law, mostly in regard to public order or justice administration.

The Constitution contemplates the figure of *Habeas Data*, a constitutional resource that provides an individual with the right to be informed and aware of the existence and have access to files related to their personal data or data about their properties despite having been stored in private or public files and in any form. Moreover, establish the right to know the use and purpose, the source and destiny of such data and the time it will be held in those files.

Both the Ecuadorian and Argentinian Constitution guarantee the right to personal data protection, contain several dispositions in regard to such data that constitute the basis for the creation of laws necessary to ensure the protection of these rights and provide the figure of *Habeas Data*.

2.2.1 *Habeas Data* in Ecuador: Background, definition, scope and application

2.2.1.1. Background and definition

Habeas Data is a relatively new figure of constitutional guarantees in the National Legislation, as its first appearance was in the Constitution created in 1996. However, the definition and scope of *Habeas Data* is wider in the current *Magna Carta*, considering that it has been changed two times since the first appearance of the figure. The word *Habeas* has

[129] Aldunate, Luz. (1998) La Fuerza Normativa de la Constitución. Revista Chilena de Derecho Número Especial p. 137-139
[130] Political Constitution of the Republic of Ecuador 2008 Art 66. 11)
[131] Political Constitution of the Republic of Ecuador 2008 Art 66. 19)

its origin in the Latin language, meaning conserve or safe. Data as we know stands from information.[132] Also, before the incorporation of the figure of *Habeas Data* the *Habeas Corpus*,[133] already existed in many constitutions including the Ecuadorian many years before. In this case, the legal action refers to *saving* the *corpus* or body instead of data, applicable to cases where a person has been imprisoned and requires to be brought in front of a Judge or authority.

The definition of a constitutional guarantee should be brought out. A constitutional guarantee is known as the set of tutorship mechanisms that are intended to ensure and strengthen the enjoyment of fundamental rights,[134] such as *Habeas Data*. Julio Cesar Trujillo, a recognized Ecuadorian lawyer and professor defined *Habeas Data* as "A Legal Precept accessible to the human being for the defense of their rights in a situation of danger or that had been illegally restricted".[135]

The constitutional resource of *Habeas Data* can be practically understood, in the words of Enrique Falcon, as "the urgent medicine to obtain personal information".[136] Falcon call it "urgent" based on the fact that it's a constitutional guarantee, which in means of the Constitutional Principle of Direct and Immediate Application contemplated in the Article 11 of the Constitution, the disposes that the rights and guarantees establish in the text are applied directly and immediately by and against *any* public servant.

To define what *Habeas Data* judicially means more than what it is for or from were the words come from, it can be said that it is a constitutional guarantee that every human has to request by judicial means the access to all the private and public records that include their personal data or their family members personal data, in order to be informed about its existence, accuracy and be able to request rectification or the suppression of the data that imply

[132] Alvarado, Karla. (2004) El Habeas Data Como Garantía de Protección De La Persona Frente al Tratamiento De Sus Datos Personales. p. 101-103
[133] Habeas Corpus: Constitutional guarantee that requires a person who has been arrested or imprisoned to be brought to a judge or into court.
[134] Lovato Gutierres, Roberto (2005) El hábeas corpus y el habeas data como garantía de los derechos fundamentales
[135] Trujillo Vásquez, Julio César. (1994) Teoría del Estado en el Ecuador, Estudio de Derecho Constitucional; Corporación Editora Nacional, Editorial Ecuador, Quito, página 100
[136] Falcon, Enrique (1996) Habeas data: Concepto y procedimiento. p. 23-24.

discrimination.[137]

Jurisprudence from the Constitutional Court of Ecuador[138] has created jurisdiction in regard to *Habeas Data*. The decision No. 182-15-SEP-C[139] declares that *Habeas Data* is the constitutional guarantee that allows natural and legal persons, to access the information about themselves stored in a public or private registry or database, with the purpose of knowing the content of such information and if the following is the case, demand its update, rectification, elimination or annulation when such information are causing some kind or harm, for the purposes of safeguarding their right to personal and family privacy. Ecuador recognizes the legal figure of *Habeas Data* as a Constitutional guarantee that involves several rights related to personal data protection. Argentina recognized the same rights but under the name of "*amparo*", which is translated to shelter.[140]

2.2.1.2. Scope of Habeas Data according to Article 92 of the Constitution and its application

Habeas Data as mentioned before, is a set of guardianship mechanisms to ensure the execution of fundamental rights. Therefore, it is a fact that there are several rights that are channelized through *Habeas Data*. The number or names of the rights can be variant from one jurisdiction to another, but it always complies with its spirit, which is to be a tool to exercise the right to privacy and the protection and access to personal data.

Alberto Bianchi, an Argentinian constitutional law lawyer, states that *Habeas Data* is based in the right to privacy, honor and identity[141]. Moreover, and in relation to the Ecuadorian legislature, other authors sustain that the constitutional guarantee includes the rights to identity, privacy, intimacy, personal data protection and informative auto determination.[142] All included in the Article 92 of the Constitution that is exposed below.

---

[137] Ekmekdjian, Miguel Angel y Calogero, Pizzolo. (2003) Habeas Data, "El Derecho a la Intimidad frente a la Revolución Infromática" p.2-3.

[138] Constitutional Court of Ecuador, Highest organ of control, constitutional interpretation, and justice administration in this matter according to Article 429 from the Constitution of Ecuador 2008

[139] Jurisprudence quoted in the thesis from Granja Villa, Jennifer (2019) "Portección de Datos Personales y Habeas Data ecuatoriano en la Era Digital" Universidad Central del Ecuador

[140] Constitution of the Argentine Nation 1853 Article 43

[141] Bianchi, Alberto. (2001) Las acciones de clase, Ábaco, Buenos Aires 135

[142] Basterra, Marcela (2005). La garantía constitucional del habeas data. En AAVV: Derecho Procesal Constitucional; Editorial Universidad, Buenos Aires p.141/186

According strictly to the Article 92 of the Constitution, *Habeas data* is a guarantee that assures to the individuals many rights related to personal data[143], expressly such as the right to be informed about the existence of the database, files or documents that contain individuals personal data, or information of their assets with no cost despite of been hold by a private or public entity; know the purpose, source and destiny, the time it has been or will be in those files or database; give consent for their personal data to be publicly disclosed; request the: update; rectification; erasure or annulation of their persona data.

Moreover, as mentioned before, *Habeas Data* per se contains a diversity of rights. Marcela Basterra defines that this constitutional guarantee includes the rights to intimacy, privacy, identity, personal integrity and informative auto determination.[144] Based on the Ecuadorian Law, the tutorship mechanism of *Habeas Data* is viable when: 1) the access to the files containing the individual personal data is denied; 2) when the request to update, rectify, deletion or annulation of wrong or harmful data is denied and; 3) when the use of the personal data violates a constitutional right without the personal data owner consent or by law or judicial order.

The process of *Habeas Data* is divided in four stages: the case submission, the qualification of the plaint by the Judge of the Court that admits the case,[145] the Audience with the parties involved (plaintiff and defendant) and finally the judgment, which is susceptible of an appeal.[146] Strictly following the time frames imposed by the law, counting since the case was submitted to the date of the judgment there should be no more than four days. However, the reality is that this process can take more time, as in the example we bring up now.

In the case 0001-15-HD from the Constitutional Court of Ecuador,[147] Jose Manuel Sanchez presents a case against Diners Club in regard to documents from a different case that this company claimed to have and its access was denied to the plaintiff.

---

[143] Political Constitution of the Republic of Ecuador 2008 Art. 92

[144] Basterra, Marcela (2005). La garantía constitucional del habeas data. En AAVV: Derecho Procesal Constitucional

[145] A constitutional right can be claimed in any Court of any matter and or level.

[146]. Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Art. 8

[147] Case 0001-15-HD from the Constitutional Court of Ecuador. Jose Manuel Sanchez Cajas Diners Club Del Ecuador S.A. https://portal.corteconstitucional.gob.ec/FichaCausa.aspx?numcausa=0001-15-HD

The lawsuit was presented on August 29, 2008 and the judgment from the court came on October 14, 2008. Already more than the 4 days promised by the law. However, the plane was denied by this court and then appealed by the plaintiff to the Constitutional Court, where it was denied again in March 2019. Meaning that an individual in pursuit of claiming his right to data protection or in this case access to information that contains his personal data will require to wait at least 3 months for a first answer and if it is denied, fight and wait for ten more years.

In conclusion, *Habeas Data* aims to cover and guarantee the access to justice and repair of the rights directly or indirectly related to it and currently, is the only mechanism that Ecuador legal framework offers to claim personal data protection and privacy rights. This mechanism lacks efficiency and has become obsolete.

2.3. Ecuador International Agreements in relation to the Protection of Personal Data

As a replacement or band aid for the lack of personal data protection regulations in Ecuador, the country, as member of commercial and political organizations with other States, has become part of several International Instruments regarding data protection and the transfer of such data.

International agreements occupy the second level in the hierarchy of the norm in Ecuador, just under the Constitution. Meaning, as explained before, that the regulations prescribed in the International Instruments that Ecuador has adhered too, have validity and are applicable in case of a prejudice to the rights comprehended in those agreements, covering when needed the lack of national legislation over a certain matter, in this case, the protection of personal data. Nonetheless, most of them have the category of directive, so despite having been an international instrument, it lacks strength to be enforced.

To evoke the most relevant of the treaties regarding data protection. However, none of them include the protection of this data when it is transferred abroad. Ecuador is part of: The European Convention on Human Rights (ECHR), which contemplates the right to privacy; American Declaration on the Rights and Obligations of Men, subscribed in Colombia, 1948,

that recognize the right to personal data and its correct treatment, and; the Organization of Economic Cooperation and Development, that includes the right to intimacy in 1980.

In 2003 countries representatives from different continents gathered in Antigua Guatemala for the second Iberoamerican Meeting for the Protection of Data.[148] As a consequence, in a cross governmental effort, the Iberoamerican Data Protection Network was created.[149] The objective of this Network in relation to the protection of personal data is to create directives for the harmonization of personal data protection across *Iberoamérica*. All of the members have in their national legislations the guarantee of the previously voiced *Habeas Data*, however, the constitutional right must be accompanied and integrated by a legal framework within the national legislation aiming to be uniform and harmonized with the rest of the Network in order to ensure an equivalent level of personal data protection. Ecuador is part of the cited Network only as an observer, so the guidelines issued by the Network and the Meetings are a mere directive. Even the representative for the country is the Function of Transparency and Social Control,[150] which has no functions related to data protection according to the ones provided to the Constitution of 2008.

To bring up a current and relevant international agreement, Ecuador subscribed a Multiparty Trade Agreement with the EU (The Agreement), with the objective of improving the framework and conditions of the exchange of goods and services between the EU member countries and Ecuador.[151] It should be brought up that Ecuador paused the negotiations with the EU in 2009 and got back to them in the end of 2016 when Peru and Colombia where already subscribed and ratified, therefore, Ecuador subscribed an adhesion to the mentioned Multiparty Agreement

[148] Encuentro Iberoamericana de Protección de Datos 2003, Antigua Guatemala, Guatemala. https://www.redipd.org/es/actividades/encuentros
[149] Red Iberoamericana de Protección de Datos 2003. https://www.redipd.org/es/la-red/entidades-acreditadas

[150] Article 5 of the Political Constitution of Ecuador 2008. https://www.cpccs.gob.ec/
[151] Trade Agreement between the European Union and its Member States, of the one part, and Ecuador, of the other part.https://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=11284

The Agreement contains several dispositions in regard to the protection of personal data. For the purposes of the Agreement it defines personal as "any information relating to an identified or identifiable individual". It also suggests that this concept may also apply if the legislation of the country disposes it.[152] It demands Ecuador to become a safe harbor[153] and also the existence of an authority specialized in the protection of personal data.[154] It assigns a working group with the duty of proposing guidelines and strategies enabling the signatory countries to become a safe harbor for the protection of personal data. The creation of the DPA will come after the publication of the law.

In regard to data processing, it dictates that "each Party shall adopt adequate safeguards for the protection of the right to privacy, in particular with regard to the transfer of personal data". Based on a disorganized and incomplete data protection legal framework that currently rules Ecuador, there are no such adequate safeguards.

In relation to the exchange of goods and services, this Agreement also mentions that the actors of e-commerce must be in constant communication in regard to incidents involving among others, personal data. In fact, it establishes that data may be exchanged only when the country receiver is compromised to ensure the protection of such data in an equivalent level as the sender.[155] Article 164 expressly demands that the subscribers "shall endeavor, insofar as possible, to develop or maintain regulations for the protection of personal data." In this case Ecuador would have to develop a data protection framework to be compliant with this mandate.

2.4. Same or Inferior hierarchy laws and regulations regarding personal data protection in Ecuador

In Ecuador there is not a single unified law that comprehends all the rights, obligations and protections to personal data. The rights and obligations that the current legislation provides are dispersed among many different laws regarding distinct matters. There can be found

[152] Ibid. Art. 1
[153] Agreement Art. 109 b)
[154] Ibid Art. 157 2) 162 and 164
[155] Agreement Art. 10

articles with dispositions related to personal data or the protection of such data, for instance, in the Telecommunications Law and also in the Criminal Code (COIP), making it difficult for the individuals to have access to the guarantees that ensure the protection of personal data.

To keep an order, the relevant laws and articles will be exposed according to their hierarchy; from higher to lowest. As the Constitution protections and rights were already discussed in one of the previous subchapters, it will be excluded from this one, but always considering the Organic Laws that follow derive from the dispositions of the *Magna Carta*.

2.4.1 Telecommunications Law

The most relevant law including the more rights, obligations and protections of personal data is the Telecommunications Law (LOT), which has the same hierarchy that the LPDP will have if it is approved. In its article 23, 4) it states that the individuals (clients that we can understand as data subjects) who want to contract telecommunication services are obliged to provide their personal data of identification in order to get a service[156].

Telecommunication Service Providers (TSP) also have obligations over their customers' personal data that they gather and process in the sense that they are required by law to adopt the necessary measures for the protection of personal data based on the ruling of the law and the technical norms in this regard[157].

For practical purposes the obligations of the Telecommunication companies will be exposed in a list and comparing or placing them under to or under the GDPR provisions and exclusively regarding the process, gathering and transmission of such data, excluding for instance, physical records like the phone books.

The TSP is obliged by the LOT to adopt technical measures to preserve the security of their networks and guarantee the secrecy of the communications and the information transmitted through their networks. An interception of communications is only possible when there is a judicial order regarding an investigation of national or public security.

[156] LOT Art. 23. 4)
[157] LOT Art. 24. 14)

Additionally, the Telecommunication services providers are obliged to deliver to the authorities any information required with the purpose of crime investigation according to the parameters defined by the Telecommunications Regulation and Control Agency (The TRCA).

The TSP must guarantee the protection of personal data by adopting adequate technical and administrative measures in order to guarantee the right to intimacy. They are prohibited to use their customer's personal data, information of the usage of their service, information about the traffic or consumption of their customers for the promotion of their series or products unless there is an approval and consent from the customers as expressed before.[158]

A TSP must inform their customers when there is a risk of violation of their network security and provide information about the risk and what measures should be adopted. The LOT also defines what is considered a violation of personal data. It is the violation of the securities that cause the accidental or illegal destruction, the loss, the alteration, disclosure or non-authorized access of transmitted gathered or processed personal data during the provision of a telecommunication service.[159]

Moreover, the TSP are obliged to implement internal procedures to address the personal data access requests from their customers. Moreover, these procedures should be at disposition for the TRCA. Here we find at least one mechanism to claim for personal data rights in regard telecommunications. An important element considered by the EC in Argentina and Japan adequacy decisions. However, in such cases the mechanisms were of a general applicability, contrary to the LOT, which is specific.

As per the obligations of the TSP, it can be seen that the current LOT not just disposes mandates to be complied by the TSP, but also provides rights and protections to Telecommunication service customers' personal data that derive from these obligations, even without having a proper law in force for that specific purpose. The issue would be that the law is determined to rule the TSP activity, meaning that in order for the individuals to claim

[158] LOT Art. 82
[159] Ibid.

these rights, there is the limitation on who to point responsible for a violation of personal data when it is not related to an entity considered a TSP.

This LOT also provides explicit data protection rights to the individuals using the TSP services and/or products. The rights are dispersed around the law and as mentioned before, some of them derive from obligations of the TSP, like for example the right to intimacy.[160]

The LOT prescribes rights to individuals such a right to intimacy, to be informed, secrecy and inviolability of the content of their communications, to the privacy and protection of their personal data to be provided with adequate and timely protection against the violations to the law or the agreements committed by the TSP, and access to their data to be modified or removed.
To summarize, the LOT covers a variety of rights and offers mechanisms to the protection of personal data that are contemplated in the Constitution but only in regard telecommunications, missing the existence of a specific law and a specialized protection entity as in Argentina and Japan.

2.4.2 Ecuador Criminal Law

The *Código Orgánico Integral Penal* (COIP), Ecuador's criminal law, prescribes a section of crimes against the right to personal and familiar privacy. Specifically regarding personal data, any individual who without the consent of the personal data owner or a legitimate reason, access, intercepts, examine, retain, record, reproduce, disseminate or publish personal data, should be punished with one to three years of imprisonment, except for those who are part of the audio and video recordings that were published and if the discussion is about public information.[161]

For an individual who´s right to privacy has been possibly perpetrated, in order for them to access justice or have a restitution of the original state of their right to privacy, as it is cataloged as a crime, it is needed to follow the procedures established by the law. The affected must submit the relevant denounce against the Prosecution, which is the entity in charge of investigating crimes.

[160] LOT Art. 78
[161] Código Orgánico Integral Penal Art. 178

As an example, we can use a viral case of violation to privacy in Ecuador. A man records a video of his wife and her boss on their way out of a motel. The woman was a public servant at the time, and as the video became viral the personal information of the woman was disclosed. Her full name, place of work, names of her children and other elements considered as personal data were also known by the public.[162]

Due to the lack of regulations or clear concepts, there were divided opinions on who was the criminal in this case; if the man who recorded the video or the person who disclosed it. It was also said that the disclosure of this video meant philological violence against the woman, which is another crime consequence of the divulgation of her personal data to the public.[163]

In this particular case, the prosecution did not initiate an investigation as the article of intimacy violation in the COIP makes the exception to those cases when the other person (supposed criminal) is also in the video or recording, as in this situation.

On the other hand, different lawyers suggested an alternative for the violation of intimacy, suggesting the victim to denounce the commission of the contravention of uttering expressions in discredit or disgrace against another instead.[164]

In 2017, secret hidden video cameras were found in Ecuador's Presidential office after 4 months of the mandate of the President Lenin Moreno,[165] who cataloged this as a violation of his intimacy. Julio Cesar Cueva, an Ecuadorian criminal lawyer, stated that "Placing a camera in the presidential office is a crime of violation of privacy. The articles 178, 180 and 233 of the COIP had been violated."[166] The article 178 prescribes the crime of the violation

[162] El Universo 2017 "Violación a la intimidad, entre delitos por difusión de videos en redes sociales" https://www.eluniverso.com/noticias/2017/03/12/nota/6084508/violacion-intimidad-delitos-difusion-video
[163] Ibid.
[164] Ibid.
[165] BBC: Una cámara oculta en el despacho presidencial: la nueva disputa entre el presidente de Ecuador, Lenín Moreno, y su antecesor Rafael Correa https://www.bbc.com/mundo/noticias-america-latina-41291012

[166] El Universo 2017: "Juristas ven una violación a la intimidad por cámara hallada en el despacho presidencial" https://www.eluniverso.com/noticias/2017/09/16/nota/6383020/juristas-ven-violacion-intimidad

to privacy, as mentioned before, However, the other two articles that Cueva evokes; 180, which prescribes the disclosure of information of restricted circulation and 233, that disposes the crimes against public information legally reserved.[167]

Moreover, the local newspaper *El Universo*[168] quoted that in order to determine if this act was a crime, it was necessary to prove the purpose of the camera being installed. It needs to be established if the camera was installed with the purpose of spying in order to fit this behavior in a criminal conduct. No further action was taken in this case and none of them was elevated to a criminal court.

As per both examples, we can see that the guarantee and protection to the right of privacy and personal data given by the COIP is far from the citizens and victims scope. The time it takes to amend a violation of privacy or personal data protection from the moment of the perpetration to the judgment of the court is too long. The access to the protection of personal data using criminal procedures is not immediate.

2.4.3 Ecuador Public Data National System Law and Public Data Registries

In Ecuador there are several public data registries for natural and legal persons. In these registries an individual should enroll the information of their property such as cars and real estate. In these public data registries ruled by the Public Data National System Law (PDNSL) it is possible for anyone to request information about an individual asset, with or without their consent. For instance, any person can file a request and pay a fee in the Property Registry to obtain a third person, natural or legal, list of real estate and its information. According to the article 41 of the national Registry Law,[169] it is mandatory to register certain information of a real estate, being the most relevant the names, surnames and domicile of the parties or owners of the property; the nature and date of the property title and the name and boundaries of the property.

[167] COIP articles 180 and 233

[168] El Universo 2017: "Juristas ven una violación a la intimidad por cámara hallada en el despacho presidencial" https://www.eluniverso.com/noticias/2017/09/16/nota/6383020/juristas-ven-violacion-intimidad

[169] Registry Law. Ley de Registro Ecuador https://www.gob.ec/index.php/regulaciones/ley-registro

The Registry Law defines that the names of the owners, holders, beneficiaries and all those who are holders of any rights over shares, participations, beneficiary parties or any other corporate title generated by a commercial or civil entity constitute public information and may be requested by any individual.[170] However, the modification, deletion and rectification of the data can be done only under the data subject exclusive request or a judicial order. As a consequence, it is also accessible for any individual to see the complete information of a company including the full names and National ID numbers of their shareholders and directors. By visiting the Companies Superintendence web site, the access to personal data only requires to know the name of the company.[171]

All the data stored is susceptible to be transferred to other public institutions that require such information based on the requirements of other laws. The PDNSL disposes that the information should be shared with other public institutions when these transactions do not violate any law disposition. The entity created by the PDNSL, named the Direction[172], and has the duty to organize a system for the transfer of personal data among public entities.

2.4.4 Communication Law

The Ecuadorian Communication law[173] does not contain a relevant number of dispositions in regard to the protection of personal data. However, it does provide an important disposition regarding the restriction to the circulation of information and also in relation to the personal data that communication companies must gather when there is space on the bottom of a note in the web page destined to collect and display people's comments on the article.

The norm specifies that the free circulation of personal data and the data consequence of personal communications is fully restricted especially through the media. This provision protects the personal data and the content of the communication of individuals from being published or disclosed by any communication company. Furthermore, the media companies are responsible for gathering the personal data of the people who comment or interact in their platform or web site. They are obliged to have identified the people interacting in their web site and news articles. The companies can be civil, administrative and even criminal

[170] Registry Law. Ley de Registro Ecuador General Dispositions, Second.
[171] Superintendencia de Compañías https://www.supercias.gob.ec/portalscvs/
[172] Dirección Nacional de Registro de Datos Públicos Ecuador Art. 22 - 25 https://www.dinardap.gob.ec/
[173] Ley Orgánica de Comunicación. Communication Law Art. 20 and 30

responsible for not complying with this disposition. It can be understood that there is a law with a disposition with the objective of protecting personal data of individuals against the media companies.

2.5 Current situation of the transmission of data from and to Ecuador

Across the Latin American countries, there are remarkable differences between the regulations over the cross border flow of personal data and its restrictions from and to other countries of the region. Argentina, Mexico Uruguay and Colombia are some of the Latin American countries that apply restrictions and special dispositions that provide specific conditions to the national or cross border transfer of their national's personal data. Argentina for instance has implemented processes for the export of data to third countries, such as agreements and corporate binding rules.[174]

As Ecuador at present does not have a data protection law, there are no restrictions or conditions for the cross border transfer of personal data. None of the Ecuadorian laws previously exposed even mention the flow of personal data to or from third countries. The absence of a specialized data protection law is affecting the progress and evolution of the Trade Agreement between the European Union and Ecuador brought up in previous subchapters. Therefore, in addition to the existent constitutional obligation, Ecuador has an urgency for a law that is compliant with the European GDPR framework.

2.6 Comparison between the General Data Protection Regulation and Ecuador´s Project of the Organic Law for the Protection of Personal Data

Betwixt the motives described in the LOPDP to sustain the necessity of a data protection law, it is pointed out that the GDPR "affects all the countries of the world" as it "allows and incentives" that only countries with adequate level of data protection can process European citizens personal data.[175]

[174] OCDE/BID (2016), Políticas de banda ancha para América Latina y el Caribe: un manual para la economía digital, OECD Publishing, Paris. http:/dx.doi.org/10.1787/9789264259027-es p. 447.
[175] LOPDP. EM p. 3

In order to determine if the LOPDP dispositions abide within GDPR legal framework, these two norms relevant concepts and dispositions will be compared. It should be brought up the fact that the LOPDP that is subject of analysis for this work is a first draft submitted to the National Assembly and has not been discussed by it. After its submission the project of law needs to follow the procedure described in the Constitution, which contains two debates before the project becomes a law in force.[176] Therefore, the submitted LOPDP that has been studied is still susceptible to modifications.

2.6.1 Personal data definition

The GDPR definition of what is considered personal data is way wider than the one given by the Republic of Ecuador legislation. The European regulation defines personal data as information that, directly or indirectly can be used to identify an individual, including online factors like IP addresses, cookies and digital trace, location or any information that could identify a person.

The concept of Personal Data, according to the GDPR was exposed in previous subchapters when comparing it to the DPD concept. The current definition given to personal data by the legislation of Ecuador was also previously exposed. However, as the matter of this work is in regard to the LOPDP, we will discuss this potential new law definition of personal data. The LOPDP defines personal data as any information associated or possibly associated to one or more identified or identifiable individuals such as: name and last names, date of birth, address, email, phone number, national ID number, car registration, patrimonial and or educational information or any other information linked to the personal data owner identity.

Comparing Ecuador and GDPR definitions, it can be seen that the concepts are very similar. The main difference relies on the description of the specific elements that can make an individual identifiable, and Europe chose to set categories that may include the elements considered in the Ecuadorian legislation.

[176] Constitution of the Republic of Ecuador 2008 Section III Articles 132 to 140.

2.6.2 Principles for the processing of personal data

Both the GDPR and the LOPDP establish principles for the processing of personal data. The first appoints six principles which are prescribed in its Article 5. On the other hand, the Ecuadorian regulation enlists several principles in the Article 8 and describes the objectives of each of them in several articles immediately after.

The two regulations include the principles for the processing of personal data. However, the Ecuadorian LOPDP includes more principles in this list. Both regulations concur in the following: of lawfulness or legality, fairness and transparency; purpose limitation; data minimization; accuracy storage limitation, integrity and confidentiality.

Ecuador adds to the above the principles of consent; personal data security; proactive and demonstrated responsibility, favorable application to the *titular*.[177] The GDPR does not consider consent as principal per se, but as part of a lawful processing of personal data in article 6.

Consent is defined in the Article 14 of the LOPDP as the manifestation of the will of the data subject for its data to be processed and establishes the same conditions for consent as the Article 7 of the GDPR.

Moreover in regard personal data security; proactive and demonstrated responsibility, and; favorable application to the data subject, they are solely some of the obligations that the responsible for the processing of personal data have according to the LOPDP[178] but that the national legislators have included as principles.

2.6.3 Rights of the data subject

Chapter III of the LOPDP aggregate, organize and unify the rights of the data subjects that currently the Ecuadorian national legislation has dispersed among different laws for different purposes. In dispersion through the rights comprehended in both the GDPR and the LOPDP we can find: communication and transparency; information and access to the information by

[177] Art. 4 LOPDP. Titular: Natural person data subject. An intervenient subject according to Article 6 of the LODPD.
[178] Articles 18, 19 and 20 of the LOPDP respectively

the data subject; portability; rectification; erasure and right to be forgotten.

In addition, the two compared norms prescribe the right to restriction of processing, named in the Ecuadorian legislation as the right of opposition. In this case, unlike the LOPDP, the GDPR provides a list of limited scenarios when the right to restriction can be applied by the data subject. For instance, when the processing is unlawful or if the controller does not need the data because its purpose is fulfilled. The right to restriction in the LOPDP mentions that this right can be applied especially in cases of marketing, valuations or automated decisions. It does not limit the cases when a data subject may request a restriction of their data, which might create confusion when exercising the right in practice.

Following, the LOPDP disposes general exceptions to the right of rectification, actualization, erasure, and restriction. The appliance of these rights do not apply, for instance and specifically in the case of the restriction of personal data, when there is a private agreement in between that needs to be honored by the data subject and therefore the request is not appropriate. As a consequence, we can see that there is a difference between the right to restriction and its applicability, as in Ecuador it is not clear if the restriction proceeds when there is no need for the processor or controller to hold the data.

Like the GDPR, Ecuador also makes an exception to the application of all the rights provided by the LOPDP, however, it is significantly reduced compared to Europe´s GDPR. The Article 37 of the Ecuadorian project of law disposes that the rights in this law do not proceed when there is another law regulating the processing of personal data in relation to freedom of expression, risk management, natural disasters and national security. However, the data subjects can apply the other rights provided in the supplementary laws.

2.6.4 Controller and Processor

Both normative bodies contemplate the figures of data controllers and processors. In the LOPDP the controller is named as the responsible for the processing of data, which is the public authority (natural or judicial), that is responsible for the implementation of appropriate technical and organizational measures to guarantee and be able to demonstrate that the data processing is managed in compliance with the law.

According to the European GDPR, a controller is a public authority which alone or together with other public authorities or bodies determines the purposes and means of the processing of personal data.[179] On the other hand, the LOPDP does not define the data controller. However, there is a definition for the responsible of personal data, which is a natural or legal person, private or public, in charge of making decisions over the purpose and processing of personal data. It is not clear how a private entity can be an authority with the power to decide over the purposes for processing of personal data.

In the two norms the controller is obliged to "implement appropriate technical and organizational measures", policies and a code of conduct to assure and be capable of proving that personal data processing is executed obeying the law. The LOPDP includes sixteen obligations for the data responsible or controllers, which include the mandate to implement audit and verification procedures and perform security evaluations previous to the processing of personal data by the data processor. It is not defined how these obligations should be accomplished, as there is still a need for a ruling to the LOPDP, which is the norm that explains its application.

The EU the data controller is equivalent to the data processing responsible mentioned in the LOPDP, with the difference that for now, the Ecuadorian responsible for the process of data might be a public or private entity. A point to address during the discussions or debates of the project of law in the National Assembly.

In regard to the data processor, the definition from the GDPR and in the LOPDP are harmonized. The first includes in its concept that the processor can be in fact a natural or legal, public or private that processes data on behalf of the controller. The second uses the term "any person" to generalize what the GDPR is specifying. The obligations are listed in the article 72 of the LOPDP. There are twelve explicit obligations, however, there is also the disposition to consider all the other obligations prescribed by other laws, for instance, the telecommunication laws and the obligations of the Telecommunications Service Providers.

The LOPDP also disposes of infractions committed by both, the controller and/or the processor. The infractions are divided in two, slight and severe. For instance, a slight

[179] GDPR Art. 4 (7)

infraction of the data processor would be to not contribute to the audits carried by the controller or the auditor authorized by it. A severe infraction from the processor is not to implement mechanisms to maintain the confidentiality, integrity and security of personal data[180].

2.6.5 Personal Data Protection Authority

The Ecuadorian project of law creates the Data Protection Authority (DPA), which is the administrator entity responsible for the supervision, control and evaluation of the activities carried by the responsible and the processor of personal data.[181] As mentioned in the subchapter regarding the International Agreements Ecuador is part of, the EU Multilateral Agreement requires specifically to create an entity that would act as authority and would be specialized in the protection of personal data.

Among the attributions and functions of the administrator entity is to carry the supervision, control and evaluation of the activities performed by the data controller and processor. They are in charge of establishing the standard rules for data protection and also to acknowledge and resolve the claims submitted by data subjects and also to impose the sanctions that may correspond according to the infractions contained in the LOPDP. Currently there is no authority capable of resolving administrative claims over data protection. The existence of an entity that guarantees the protection of personal data is one of the requirements of the article 45 of the GDPR in order to consider a third country as offering an adequate level of data protection.

The DPA also is responsible of acquainting the claims of the data subjects. The LOPDP establish a free of charge administrative procedure in other to make their petitions effective especially those related to the access, rectification, update, erasure and other rights proper of the data subject contained in this text.[182]

[180] Ecuador. Proyecto de Ley Orgánica de Protección de Datos Personales Art. 81 and 82.
[181] Ecuador. Proyecto de Ley Orgánica de Protección de Datos Personales Art. 88.
[182] LOPDP Art. 73

2.6.6 Personal Data Security

The GDPR disposes that data controllers and processors should provide proper technical and organizational measures in order to guarantee an appropriate level of security. The personal data security measures are the following:

a) Pseudonymization and encryption: A pseudonym is defined as "an identifier of a subject other than one of the subject's real names".[183] Pseudonymization is considered an efficient armor for privacy and prevention for violations to it.[184] Pseudonymization gives the data subject protection to their sensitive information against data controllers and processors, as it allows them the possibility to create "structural correlations" with the data but with no access to personal and sensitive data. It is a convenient means to protect personal data and sensitive information.[185] Encryption can be defined as a digital process of transforming data expressed in readable text into a code supposedly impossible to decipher with no decryption key.[186] This technology is capable of offering solutions to data security challenges and can be applied to ensure a solvent security.[187] On the other hand, the LOPDP also contemplates security measures such as encryption and anonymity.[188] It should be brought up that the before mentioned figures do not exist in the current legal framework for the protection of personal data in Ecuador.

b) Ensure confidentiality, integrity, availability and resilience of processing systems and services: Confidentiality is defined by the Oxford dictionary as "a situation in which you expect somebody to keep information secret".[189] In a data protection context, the

[183] Pitzmann, Andreas. Hansen, Marit. (2010) A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management p. 21
[184] M Jawurek, M Johns, K Rieck (2011) Smart Metering De-Pseudonymization. Proceedings of the 27th Annual Computer Security Applications Conference p.227
[185] Haber, S., Hatano, Y., Honda, Y., Horne, W., Miyazaki, K., Sander, T., Tezoku, S., Yao, D.: (2008) Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. In: ASIACCS 2008, pp. 353. ACM, New York
[186] Internet article: What Is Encryption And How Does It Work? https://pixelprivacy.com/resources/what-is-encryption/
[187] Gafoor Deshmuk, Anwar Pasha Abdul; Qureshi, Riyazuddin. (2011) IJACSA International Journal of Advanced Computer Science and Applications, Vol. 2, No.3,
[188] LOPDP Art. 50; 1.
[189] https://www.oxfordlearnersdictionaries.com/definition/english/confidentiality?q=confidentiality

regulation demands the data controllers and processors to implement measures and mechanisms that ensure the confidentiality of the personal data provided by the data subject.

c) Ability to a fast restoration of availability and access to personal data when facing physical or technical incidents: The availability and access to personal data should be at hand not only when facing challenges or emergencies but continuously, as disposed by the article 66 of the Constitution, the telecommunications law and the LOPDP, as cited in previous sub chapters.

d) Processes for the testing and evaluation of technical and organizational measures that ensure the security of personal data processing: Dissimilar to the GDPR, the LOPDP does not dispose to evaluate the measures but to implement actions with the purpose of improving the technical, physical, administrative, organizational and legal resilience.[190] Additionally the GDPR contains more dispositions in regard to the measures to be performed by the controllers and processors for the security of data processing. It requires a level of security considering factors like the risk of processing, adherence to a code of conduct and ensuring the workers of the controllers and processors only process the data when instructed or required by law.[191]

2.6.7 Data protection officer

The GDPR includes the figure of the data protection officer, who is a professionally prepared person in the field of data protection that must be designated by the controllers and processors in the cases where the processing is executed by a public body except for those part of the judicial system; their main activity is to processing that need a routine and automatic monitoring of data subjects, and; large scale of special categories of data defined in this same regulation[192]. This same text even defines the parameters of the data protection officer position and their tasks.

[190] LOPDP Art. 50; 3)
[191] GDPR Art 32; 2) 3) 4)
[192] GDPR Art. 37; 1) 5)

On the other hand, the LOPDP disposes a personal data protection delegate, which would be the equivalent of the officer. Both the GDPR and LOPDP establish the same scenarios when there shall be a data protection officer. However, the Ecuadorian text disposes one more case and includes the processing of data related to national security and the State defence.[193]

Personal data protection officer's role can be resumed as being the middleman between supervisory and public authorities and other organisms of the State, data subjects and businesses.[194]

2.6.8 Transfer of personal data abroad

Overwriting completely the current framework over the transfer of personal data abroad described in previous subchapters, the LOPDP is completely harmonized with the GDPR rules. LOPDP now explicitly prescribes that it is possible to transfer personal data abroad if the conditions are satisfied. The LOPDP defines the same criteria to declare an adequate level of protection of countries and organizations that should be issued by the DPA. Moreover, it imitates the GDPR disposition over the transfer of personal data to countries with and without an adequate level of data protection, including the additional appropriate safeguards the same corporate binding rules and exceptional cases for the transfer of personal data abroad.[195]

It is also disposed by the LOPDP that it shall be implemented a continuous control by the DPA together with the academy, not specifying if national and or foreigner, to make regular reports regarding the international reality of data protection in order to determine which countries and or organizations are offering an adequate level of data protection. It does not include the observation of other international organizations like the EU, however, the academy has referred to the GDPR and its dispositions on numerous occasions.

Moreover it disposes to have an update list of those countries and organizations that have an adequate level of data protection and also issue resolutions of not complying with the adequate level decision anymore. In a general perspective it is clear that the LOPDP is

[193] LOPDP Ecuador Art. 58; 4)
[194] Cliza, Marta Claudia; Spataru, Laura Cristina (2018) The General Data Protection Regulation: what does the public authorities and bodies need to know and to do? The rise of the data protection officer Volume 8, Issue 2 p. 500
[195] LOPDP Capitulo VIII

following closely the dispositions given by the GDPR in regard to the transfer of personal data abroad and the requirements established for different scenarios depending on the country or organization acting as the receiver of such data.

3. Article 45 of the General Data Protection Regulation and Ecuador legal framework over data protection

As exposed in the previous chapter, the Article 45 2) of the GDPR sets the conditions and requirements to consider in order to determine if that third country or non-member state offers an adequate level of data protection to its citizen's personal information and therefore, also adequate for Europeans personal data.

Based on the Schrems Vs. Facebook judgment briefly exposed previously, the level of data protection in non EEA countries is found adequate when it can be considered "essentially equivalent" to the rights and protections provided by the EU.

I is a fact that an adequacy level will not be granted to Ecuador if there is no data protection law neither an authority created for its protection, therefore we will analyze if the Article 45 of the GDPR dispositions are covered by the current legal framework including the LOPDP in case it is approved with no modifications.

The Commission will consider the following elements in the Ecuadorian legal framework:

The rule of law: this concept translated to Spanish its equivalent to what in the Ecuadorian national legislature is called a State of Rights or Rights/law supremacy, or principle of "legality"[196] which means the law must be applied to everybody equally, no one is above the law and the Constitution is the superior law.[197]

In the Ecuadorian reality, despite this principle being guaranteed by the Constitution and the law, it is far from being fully respected. The application of what is prescribed in the law is what Norberto Bobbio denominated "efficiency".[198] A clear example is the existence of the

[196] https://traduccionjuridica.es/rule-of-law/

[197] Martínez Dalmau, Rubén (2008) "Supremacía de la Constitución, control de la constitucionalidad y reforma constitucional", Desafíos constitucionales, la constitución ecuatoriana de 2008, Quito, Ministerio de Justicia y Derechos Humanos /Tribunal Constitucional.

[198] Bobbio, Norberto Teoría general del Derecho, op. cit., p. 20. Quoted by Ávila Santamaría, Ramiro. (2011) El Neoconstitucionalismo transformador el estado y el derecho en la Constitución de 2008

dispositions in the Constitution regarding data protection and the non-action over it after twelve years.

Respect for human rights and fundamental freedoms: As exposed previously Ecuador is part and subscriber of the Charter of the United Nations and the Universal Declaration of Human Rights, subject to comply with the CIDH and guarantees all of the human rights contained in the Constitution. However, according to the Human Rights Watch report from 2019, Ecuador confronts "chronic human rights challenges" that include ineffective public institutions and a questionable judicial independence.[199]

According to the Preliminary Observations by the UN Special Rapporteur on freedom of expression following his visit to Ecuador in October 2018, it is suggested the autonomy of the current body acting as authority, not in regard to data protection but of the internet, by making law reforms. However, it also mentions the acknowledgement of a new data protection law, the LOPDP, despite the protection given by the Constitution.[200]

Relevant general and sectoral legislation including national security, criminal law and the access of public authorities to personal data: the lack of a specialized personal data protection was already exposed. However, the LOPDP aims to fulfil this void in the legislation.

Despite the lack of a functional data protection regulation, the current framework does include national security and criminal law dispositions in regard to personal data protection, as exposed in the previous subchapter 2.4 of this work.

The access of public authorities to personal data is covered by the law, as it establishes that every public servant can only access individuals personal information at their disposition with a judicial order and also must sign an agreement of confidentiality and are obliged to the dispositions of the DINARDAP and the law.[201] The LOPDP also limits the access to the

[199] Human Rights Watch report Ecuador October 2019.
https://www.hrw.org/world-report/2020/country-chapters/ecuador
[200] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23713&LangID=E
[201] Ruling to the access of public data Ecuador.

data subject's personal information when there is a judicial order or an authorization from the individual owner of the data.[202]

Data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country: as exposed, in the current legal framework Ecuador does not have specialized data protection rules but has some dispositions spread among different laws.

The LOT includes security measures that should be addressed in order to ensure the security of the personal data and information provided by the individuals, as described in the subchapter 2.4 in the point of the Telecommunications law. Moreover, the LOPDP includes specially designed rules for data protection and also establishes parameters for the transfer of personal data abroad, which does not exist in the current legislation.

Case-law, effective and enforceable data subject rights and effective administrative and judicial mechanisms: As exposed in the subchapter 2.2.1, the constitutional guarantee of *Habeas Data* is currently the only judicial measure to claim a constitutional data protection right that has been or can be presumably violated. With the implementation of the LOPDP and the creation of an authority responsible for ensuring the protection of personal data and the enforceability of the rights related to it, there will be an administrative, immediate and remote mechanism for data subjects to claim their rights, additionally to the judicial procedures.

Existence and effective functioning of one or more independent supervisory authorities: Currently there is one authority which is the DINARDAP. However, as it was exposed before it merely has a registry purpose more than a protection purpose and is not specialized for the protection of personal data. Its creation is not a consequence of a data protection law but a national public data registry law, focused on public information rather than sensitive or personal data of the citizens.

The LOPDP crates the DPA, entity which has the explicitly function and objective to enforce the compliance of the data protection dispositions and guarantees of the law. The emersion

[202] LOPDP Art. 47

of this authority will mean the compliance with the requirement of the EU in the Multiparty commercial Treaty brought up previously and also with the article 45 requirement.

International commitments: As mentioned in subchapter 2.3, Ecuador is committed to a considerable number of international agreements and organizations, especially the Agreement with the EU which is the most recent and relevant to this topic. It is essential to comply with its terms and develop rules for data protection. The LOPDP, based on its characteristics previously described, as it is now has shown harmonization with the GDPR definitions and mandates.

4. CONCLUSION

With its current legal framework over the protection of personal data, Ecuador is not a country that offers an adequate level protection, as it lacks of the fundamental elements that the EC considers in order to issue an adequacy decision. As per the examples of Argentina and Japan, it was consider that they provide a specific data protection law in its legislation; to have an independent authority specialized in the protection of personal data, and; to effective procedures for the data subjects to claim for the respect and protection of their data protection and privacy rights.

As per the analysis of the ruling Ecuadorian legislation in the previous subchapters, it can be established that there is no specific law for personal data protection currently in force; there is no specialized authority in regard the protection of personal data, and, despite of the possibility of interpose an *Habeas Data* and the mechanism provided by the LOT exclusively for TSP, there is no effective mechanisms to ensure the respect for personal data protection and privacy rights.

Moreover, according to the aforementioned UN Special Rapporteur suggestions Ecuador still needs to work on the protection and respect for human rights. Additionally, the Multilateral Agreement with the EU exposed in previous subchapters demands that Ecuador becomes a safe harbor and also the existence of an authority specialized in the protection of personal data. These two last provisions of the Multilateral Agreement are attempted to be complied by the LOPDP, as it was exposed that this law creates the DPA which is supposed to be the institution in charge of the protection of individual's data protection rights and, creates mechanisms for this authority to acknowledge and resolve all data subject claims.

The dispositions related to the protection of personal data that we exposed spread over the lower hierarchy regulations in the Ecuadorian legal framework that will not be affected by the approval of the LOPDP, will continue to serve as guarantees for the protection of data subject's rights and as mechanisms to ensure the protection of such rights. The regulations that currently are in force and are contradictory to the LOPDP dispositions will be repealed.

Alike in the case of Argentina, the right to data protection emerges from the Constitutional right to privacy and the guarantee of *Habeas Data*. The difference is that Argentina does have a specialized law and authority on the protection of personal data that support the constitutional provisions and ensures its applicability.

This could mean that if the LOPDP is approved as it currently is; a data protection authority is created; there are effective mechanisms for data subjects to claim their rights, and; the negotiations needed around any controversies just like Japan did, Ecuador would have an opportunity of been considered by the EC as a country offering an adequate level of data protection.

However, the approval of this law does not guarantee a favorable adequacy decision of the EC, as the article 45 of the GDPR analyzed before includes a determination of compliance with fundamental freedoms, rule of law and other elements that currently Ecuador is struggling with. Nonetheless, as in Japan case, there is space for negotiations when the national law has dispositions that are not harmonized or even go against the GDPR and also a possibility to ignore human rights controversies as far as they do not involve Europeans. For instance, Ecuador would need to ensure and promise to the EC that there will be efforts in order to increase the respect and guarantee of human rights, just like Japan and Argentina did when they had a gap between their national law and the GDPR and DPD respectively.

The Ecuadorian National Assembly should consider approving the LOPDP without major or significant modifications that affect its harmonization of data protection principles and concept as it is exposed in previous subchapters. The LOPDP should be approved as soon as possible due to the exponential digitalization the world and the social development in order to assure the protection of rights and guarantees related to the protection of personal data contemplated in the Constitution. It is necessary to count with a personal data protection law in order for Ecuador to move forward and fortify the economic, political and commercial relations with the EU. In addition, the Ecuadorian government should take action after the approval of the LOPDP and begin to negotiate with the EC the issue of an adequacy decision in favor of Ecuador.

LIST OF REFERENCES

Books

1) Michael, J., (1994) Privacy and Human Rights: An International and comparative study
2) Alexey, R. (2014) Constitutional Rights and Proportionality. Journal for constitutional theory and philosophy of law.
3) Alexy, R. 2007. *"Los derechos fundamentales en el Estado constitucional democrático"*. *Centro de Estudios Constitucionales*.
4) Davara Rodríguez, Miguel Ángel, 1998 *"La protección de datos en Europa: principios, derechos y procedimiento"*, Madrid, Grupo Asnef Equifax-Universidad Pontificia de Comillas.
5) Téllez Aguilera, Abel, "*La protección de datos en la Unión Europea"*, Madrid, Edisofer, 2002.
6) Lee A. Bygrave, 2014. 'Data Privacy Law: An International Perspective' (Oxford University Press) 1-23
7) Caillavet Chantal. (2000) Etnias del Norte: Etnohistoria e historia de Ecuador
8) Enrique Ayala Mora (1993) Resumen de Historia del Ecuador. Época Republicana Segundo Periodo Tercera edición actualizada Corporación Editora Nacional. Quito, 2008 Biblioteca General de Cultura.
9) Concha, Jorge. (1942). Eloy Alfaro: su vida y su obra. Talleres Gráficos de Educación. Quito
10) Lovato Gutierres, Roberto (2005) El hábeas corpus y el habeas data como garantía de los derechos fundamentales
11) Trujillo Vásquez, Julio César. (1994) Teoría del Estado en el Ecuador, Estudio de Derecho Constitucional; Corporación Editora Nacional, Editorial Ecuador, Quito
12) Falcon, Enrique (1996) Habeas data: Concepto y procedimiento.
13) Bianchi, Alberto. (2001) Las acciones de clase, Ábaco, Buenos Aires 135
14) Martínez Dalmau, Rubén (2008) "Supremacía de la Constitución, control de la constitucionalidad y reforma constitucional", Desafíos constitucionales, la constitución ecuatoriana de 2008, Quito, Ministerio de Justicia y Derechos Humanos /Tribunal Constitucional.

15) Bobbio, Norberto Teoría general del Derecho, op. cit., p. 20. Quoted by Ávila Santamaría, Ramiro. (2011) El Neoconstitucionalismo transformador el estado y el derecho en la Constitución de 2008

Academic articles

16) Blume, P. 2015. EU Adequacy Decisions: the proposed new possibilities. International Data Privacy Law, Volume 5, Issue 1

17) Cerda, A. 2011. The "Adequate Level of Protection" for International Personal Data Transfer from the European Union – Collection, Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, 36. Universidad Católica de Valparaíso. Valparaíso, Chile.

18) Shakila Bu-Pasha (2017) Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law

19) Blasi, C. 2015. The limits of European data protection law in EU border control. Revista CIDOB d'Afers Internacionals. n.111

20) Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya A.P. Ramanathan, Cross border data transfer: Complexity ofadequate protection and its exceptions, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.001

21) Svantesson, B. 2011. The regulation of cross-border data flows. Published by Oxford University Press.

22) Kuner, C. 2017. The GDPR as a chance to break down borders. International Data Privacy Law, 2017, Vol. 7, No. 4.

23) Tikkinen-Piri, C. 2018 EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer law & security review No. 34. University of Oulu, Finland.

24) Buttarelli, Giovanni. (2016) The EU GDPR as a clarion call for a new global digital gold standard. International Data Privacy Law, 2016, Vol. 6 No. 2.

25) Banisar, D., Davies, S. (1999) Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. The John Marshall Journal of Information Technology & Privacy Law

26) Adam D. Moore, Toward Informational Privacy Rights, 44 San Diego Law. Review. 809, 817 (2007).
27) Gross, E. 2004. The Struggle of a Democracy against Terrorism – Protection of Human Rights: The Right to Privacy versus the National Interest – the Proper Balance. Cornell International Law Journal Vol. 37
28) Cohen, J. (2013) What privacy is for. Harvard Law Review 126.
29) Hartzog, W. (2013)The fight to frame privacy. Michigan Law Review Vol. 111.
30) Simmons, J. (2001) Justification and Legitimacy: Essays on right and obligations. Cambridge University Press.
31) Garzón, Clariana, "La protección jurídica de los datos de carácter personal", 1a. Instancia. Revista de Derecho, núm. 2, marzo de 1982, p. 15.
32) Herrán Ortiz, Ana Isabel, El derecho a la protección de datos personales en la sociedad de la información, Bilbao, Universidad de Deusto, Cuadernos Deusto de Derechos Humanos, núm. 26, 2002.
33) Hallinan, Dara; Friedewald, Michael; McCarthy, Paul. (2012) Citizens' perceptions of data protection and privacy in Europe. Computer and Law & Security Review Volume 28, p. 263
34) Cate, Fred. H. (1995). The EU data protection directive, information privacy, and the public interest. Iowa Law Review 80(3), p. 431
35) Hondius, Frits. (1983) A Decade of international data protection. "Netherlands of International Law Review", Vol. 30, No. 2 p. 105-106
36) Millard, C., & Church, P., (2007a) 'Tissue Sample and Graffiti: Personal Data and the Article 29 Working Party' Computers & Law 2007, vol.18(3), pp. 27-29.
37) Perez Luño, Antonio E. (1989) Los derechos humanos en la sociedad tecnológica. CEC, p. 138-139
38) Robertson, A. H. "The European Convention for the Protection of Human Rights." British Year Book of International Law, 27, 1950,
39) Pearce, Graham and Platten, Nicholas (1998) Achieving Personal Data Protection in the European Union Journal of Common Market Studies Vol. 36, No. 4
40) Andorno, Roberto. (2005) The Oviedo Convention JIBL Vol 02
41) Simitis, Spiros (1995) From the Market to the Polis: The EU Directive on the Protection of Personal Data, 80 Iowa L. Rev. 445
42) Svantesson, Jerker B. (2011) International Data Privacy Law Vol, 1 No. 3

43) Bainbridge, David I. (1997) Processing Personal Data and the Data Protection Directive. Processing Personal Data and the Data Protection Directive
44) Gilbert, Francoise (2007) A Bird's-Eye View of Data Protection in Europe, 24 GPSolo 32
45) Hornung, Gerrit (2012) A general data protection regulation for europe? light and shade in the commission's draft of 25. SCRIPTed
46) Nikhil S. Palekar, (2008) Privacy Protection: When Is Adequate Actually Adequate, 18 Duke J. Comp. & Int'l L
47) Determann, Lothar, Adequacy of Data Protection in the EU - General Data Protection Regulation as Global Benchmark for Privacy Laws? (January 17, 2017). Available at SSRN: https://ssrn.com/abstract=2902228
48) George, Barbara (2001) et al., U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive,
49) Boyd, Virginia (2006) Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization, 24 BERKELEY J. INT'L L.
50) Wagner, Julian (2018) The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? International Data Privacy Law, Vol. 8, No. 4
51) Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya A.P. Ramanathan (2017) Cross border data transfer: Complexity of adequate protection and its exceptions. Computer law & security review
52) Gakh, Maxim. (2005) Argentina´s Protection of Personal Data: Initiation and Response.
53) Safari, Beata A. (2017) Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, 47 Seton Hall L. Rev
54) Pardis, Tehrani, Johan, Bin Hj, Dhiviya A.P. Ramanathan, 2017. Cross border data transfer: Complexity of adequate protection and its exceptions, Computer Law & Security Review: The International Journal of Technology Law and Practice . doi: 10.1016/j
55) Meyers, Anna (2016) 'Top 10 operational impacts of the GDPR: Part 4 – Cross-border data transfers' <https://iapp.org/ news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border -data-transfers/

56) Schwartz, Paul M. (2019) Global Data Privacy: The EU Way. New York University Law Review. Vol. 94:771
57) Greenleaf, Graham (2017) Questioning 'Adequacy' (Pt I) – Japan 150 Privacy Laws & Business International Report, 1, 6-11 UNSW Law Research Paper
58) Yohko Orito and Kiyoshi Murata (2005) Privacy Protection in Japan: Cultural Influence on the Universal Value
59) Aldunate, Luz. (1998) La Fuerza Normativa de la Constitución. Revista Chilena de Derecho Número Especial
60) Ekmekdjian, Miguel Angel y Calogero, Pizzolo. (2003) Habeas Data, "El Derecho a la Intimidad frente a la Revolución Infromática"
61) Basterra, Marcela (2005). La garantía constitucional del habeas data. En AAVV: Derecho Procesal Constitucional; Editorial Universidad, Buenos Aires
62) M Jawurek, M Johns, K Rieck (2011) Smart Metering De-Pseudonymization. Proceedings of the 27th Annual Computer Security Applications Conference
63) Haber, S., Hatano, Y., Honda, Y., Horne, W., Miyazaki, K., Sander, T., Tezoku, S., Yao, D.: (2008) Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. In: ASIACCS 2008, pp. 353. ACM, New York
64) Gafoor Deshmuk, Anwar Pasha Abdul; Qureshi, Riyazuddin. (2011) IJACSA International Journal of Advanced Computer Science and Applications, Vol. 2, No.3
65) Cliza, Marta Claudia; Spataru, Laura Cristina (2018) The General Data Protection Regulation: what does the public authorities and bodies need to know and to do? The rise of the data protection officer Volume 8, Issue 2

Laws and regulations

Ecuadorian legislation:

66) Ley del Sistema Nacional de Registro de Datos Públicos. Public Data National System Law.
67) Proyecto de Ley Orgánica de Protección de Datos Personales. Memorando No. PAN-CLC-2019-0184. Quito D.M, 19 SEP 2019. LOPDP
68) Ley Orgánica de Telecomunicaciones. Telecommunications Law.
69) Código Orgánico Integral Penal. Criminal Code.

70) Constitution 2008 Republic of Ecuador
71) Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Judicial guarantees and constitutional control Law.
72) Registry Law. Ley de Registro Ecuador
73) Ley Orgánica de Comunicación. Communication Law

European Union legislation:

74) Council of the European Union (1995), 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, Official Journal of the European Union, OJ L 281, 23.11.1995, p. 31–50.
75) European Commission Decision of 30 June 2003, 2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, OJ L 168, 5.7.2003, p. 19–22.
76) Council of the European Union (2016), 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, Official Journal of the European Union, OJ L 119, 4.5.2016, p. 1–88.
77) Free movement of goods, EEC Treaty art. 9, persons, id. art. 48, services, id. art. 59, and capital, id. art. 73b, as amended by Maastricht Treaty, supra note 1, art. G, 31 I.L.M. at 256. See aso Berman et al., supra note 1, at 317.
78) Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC)
79) CJEU: First Reaction to AG's Opinion on NSA "PRISM" Scandal Facebook's EU-US
80) https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421 European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows (2019)

International legislation

81) Universal Declaration of Human Rights.

82) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28/01/1981

83) Treaty No.164 Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine

84) Directive 95/46/EC Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data

85) Opinion 4/2002 on the level of protection of personal data in Argentina

86) Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina

87) Constitution of the Argentine Nation 1853

88) Trade Agreement between the European Union and its Member States, of the one part, and Ecuador, of the other part. https://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=11284

Court Decisions:

89) Case C-362/14 Maximillian Schrems vs. Data Protection Commissioner https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN

90) Law for the Protection of Personal Data, Argentina

91) Jurisprudence quoted in the thesis from Granja Villa, Jennifer (2019) “Portección de Datos Personales y Habeas Data ecuatoriano en la Era Digital” Universidad Central del Ecuador

92) Case 0001-15-HD from the Constitutional Court of Ecuador. Jose Manuel Sanchez Cajas Diners Club Del Ecuador S.A. https://portal.corteconstitucional.gob.ec/FichaCausa.aspx?numcausa=0001-15-HD

Electronic sources

Newspaper Articles:

- Curtis, S. & Hoggins, T. (2014), 'Is Destiny the most expensive video game ever made?' The Telegraph, 9 September 2014.
- Duxbury, C. (2015), 'Sweden ends military cooperation deal with Saudi Arabia: criticism of Saudi rights record causes diplomatic standoff,' The Wall Street Journal, 10 March 2015.
- Hoyos, C. (2013), 'Europe defence groups urge technology sharing,' The Financial Times, 13 October 2013.
- BBC: Data on almost every Ecuadorian citizen leaked. September 16, 2019. https://www.bbc.com/news/technology-49715478
- Press Release, European Commission, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-releaseIP-16-216_en.htm.
- El Universo 2017 "Violación a la intimidad, entre delitos por difusión de videos en redes sociales" https://www.eluniverso.com/noticias/2017/03/12/nota/6084508/violacion-intimidad-delitos-difusion-videos
- BBC: Una cámara oculta en el despacho presidencial: la nueva disputa entre el presidente de Ecuador, Lenín Moreno, y su antecesor Rafael Correa https://www.bbc.com/mundo/noticias-america-latina-41291012
- El Universo 2017: "Juristas ven una violación a la intimidad por cámara hallada en el despacho presidencial" https://www.eluniverso.com/noticias/2017/09/16/nota/6383020/juristas-ven-violacion-intimidad

Reports, working papers:

- Council of the European Union (2015), Digital Economy and Society Index 2015: Methodological note, Brussels.
- Class Action against Facebook Ireland, EUR. VERSUS FACEBOOK (Dec. 1, 2015), http://europe-v-facebook.org/EN/Complaints/Class_Action/classaction.html. quoted

in Beata A. Safari, (2017) Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, 47 Seton Hall L. Rev. 809

- Alvarado, Karla. (2004) El Habeas Data Como Garantía de Protección De La Persona Frente al Tratamiento De Sus Datos Personales
- OCDE/BID (2016), Políticas de banda ancha para América Latina y el Caribe: un manual para la economía digital, OECD Publishing, Paris. p. 447 http:/dx.doi.org/10.1787/9789264259027-es
- Internet article: What Is Encryption And How Does It Work? https://pixelprivacy.com/resources/what-is-encryption/
- Human Rights Watch report Ecuador October 2019. https://www.hrw.org/world-report/2020/country-chapters/ecuador

Other sources

- Ecuador National Assembly. Legislative Power of the Republic in charge of the creation of laws. https://www.asambleanacional.gob.ec/es
- Opinion No. 4/2007 on the concept of personal data - WP 136 (20.06.2007)
- European Commission Press Release IP/10/421, European Commission Adopts Adequacy Decision on Japan, Creating the World´s Largest Area of Safe Data Flows (Jan 23, 2019)
- Encuentro Iberoamericana de Protección de Datos 2003, Antigua Guatemala, Guatemala. https://www.redipd.org/es/actividades/encuentros
- Red Iberoamericana de Protección de Datos 2003. https://www.redipd.org/es/la-red/entidades-acreditad

Appendix Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I Stefano Roggiero,

1.Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

Ecuador as a country with an ´adequate´ level of data protection.
(title of the graduation thesis)

supervised Anni Säär,
(supervisor's name)

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*