UNIVERSITY OF TARTU
SCHOOL OF LAW
Department of Public Law

Mario Antonio Alfaro Bobadilla

The Right to Data Protection in the US: The influence of GDPR in the US Model

Master's Thesis

Supervisor
dr. iur. Paloma Krõõt Tupay

Tallinn, Estonia 2019

TABLE OF CONTENTS

INTRODUCTION

We live in a society that is continuously evolving, and technologies change daily. We accept certain risks without really realising what they imply. In this sense, we accept the need to deliver our personal information to companies that presume that they can keep our information secure for an indeterminate time, under any circumstances, and that they will not sell our personal information to the highest bidder. It is unknown to anyone that every time we fill out a form, sign a contract, or accept the terms and conditions of a product we are delivering personal information that companies can use in various ways. The information delivered to different services is used in diverse ways that can damage our physical and spiritual/digital integrity. Usually, when we access certain services, we will realize that we are delivering personal data of a different nature to certain institutions that can use this information to harm us. Today, not only are we exposed to a simple invasion of privacy, but we can also be exposed to identity theft, online fraud, companies are monetizing with the collection of your personal data, or worse, influence in the political decisions of each person through the collection of private data[1].

Today, the services that people use in society have taken the privacy of each person to a terrain in which the vulnerability of a person's data has increased considerably. One of the most common cases has to do with social networks. Social networks can be referred to as "a virtual community or profile site; a social network is a website that brings people together to talk, share ideas and interests, or make new friends. This type of collaboration and sharing is known as social media. Unlike traditional media that is created by no more than ten people, social media sites contain content created by hundreds or even millions of different people."[2] Every time we use a social network service, we are accepting tacitly that our privacy is being violated whenever there is an intermediary for the transfer of our information. What is more, all the content we upload to our account on social networks becomes social data, in this sense, it is possible to understand social data such as our geographical location, our language, the links we share, etc. This brings with it a series of consequences since this data is very precious for marketing companies that seek to generate a profit in sales.

[1] BBC Mundo. (2018) 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. BBC. https://www.bbc.com/mundo/noticias-43472797

[2] Computer Hope. (2019). Social network. Computer Hope Free computer help since 1998. https://www.computerhope.com/jargon/s/socinetw.htm

The right to privacy is an essential element of each legal system, and it can be both nationally and internationally which the main objective is to curb the actions of the state and private parties that threaten the privacy of individuals[3]. Privacy is an ambiguous concept that can be interpreted differently depending on the culture, but it is possible to interpret it as the ability of individuals to isolate themselves as persons or to isolate information about them, and therefore selectively disclose it to other individuals. The right to privacy is recognised in the Universal Declaration of Human Rights ("UDHR"), and from this right, it is possible to derive others, such as the Right to Data Protection. The right to data protection as a right derived from the right to privacy is possible to understand as a tool that is used by the right of privacy to ensure that individuals are protected from any abuse of their personal information by another individual[4]. Although there are academics who can understand the right to data protection as a mere tool of the right to privacy, there are legal systems that recognise the right to data protection as an independent right to the right to privacy[5]. Therefore, it would be possible to talk about a duality regarding the right to data protection that has a tool function and right at the same time. To describe this duality raised above, it is necessary to understand how the right to data protection and the right to privacy is understood, specifically in the United States ("US") and in the European Union ("EU"). In the United States, the right to privacy has always been understood as an element of freedom, and it is the right to be free from state interference.[6] The academic Gavison suggests a definition of the right to privacy in which the interest in privacy is given in the fact of giving access, either physically in the invasion of one's own space, or buying private information about a person, and by both removing his anonymity.[7] On the other hand, the European Union encompasses from another point of view the right to privacy, every human being is endowed with human dignity[8], and within this human dignity, it is possible to understand that there is a right to maintain a private, autonomous life that people have control of their

[3] Warren, S. D; Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, Vol. IV, pp. 193-220.*

[4] GVZH. Data Protection vs. The Right to Privacy. GVZH Advocates. https://www.gvzh.com.mt/malta-law/data-protection/vs-the-right-to-privacy/ /

[5] Granger, M.-P., and Irion, K. (2018). 'The right to protection of personal data: the new posterchild of European Union citizenship?' in: *de Vries, S., de Waele, H., and Granger, M.-P., eds., Civil Rights and EU Citizenship (Cheltenham: Edward Elgar Pub.), 3-4.*

[6] Warren, Brandeis, supra note 3.

[7] Onn, Y. (2005). Privacy in the Digital Environment. *Haifa Center of Law & Technology. Pp 61, 68.*

[8] United Nations. (1948). Universal Declaration of Human Rights. https://www.un.org/en/universal-declaration-human-rights/. Articles 1-2

information, to be left free[9]. Privacy in the European Union is not only a right granted to an individual, but it is also integrated as a social value[10].

The author of this thesis will direct his work to understand the Privacy Law in the United States, specifically the Right to Data Protection. To conduct this work, the author of this thesis will take two models, the first model is the model of the United States in terms of privacy and data protection, and the second model is the model of the European Union in terms of privacy and data protection. To begin analysing the right to data protection in both legal systems, it is necessary to provide an understanding of how the right to privacy is conceived in the model of the United States and the European Union. Therefore, the author of this thesis before rigorously delving into the development of the right to data protection in both models will cover the right to privacy in the model of the United States and the European Union. The data protection system will be developed in the US model through various laws on data protection and its relationship with the different international treaties regarding human rights. While in the European model it is possible to draw a correlation between the right to data protection and the different international human rights treaties since the European Union consecrates data protection as a fundamental right in the article 8 European Union Charter of Fundamental Rights ("EU Charter").

It is necessary and interesting to compare the United States and European state model regarding privacy and data protection since, while the European Union makes an express reference to the right to privacy in its article 8 of the European Convention on Human Rights ("ECHR") and its article 7 EU Charter, the same does not happen in the case of the United States. Although the Constitution of the United States does not explicitly guarantee a Right to Privacy, the United States Supreme Court has made up for this omission and has made an extensive interpretation of the first, third, fourth, fifth, ninth and fourteenth amendments to guarantee the right to privacy to the citizens of the United States. Although the judges of the Supreme Court of the United States have understood that the right to privacy is implicit in

[9] Privacy International. PRIVACY AND HUMAN RIGHTS An International Survey of Privacy Laws and Practice. Global Internet Liberty Campaign. http://gilc.org/privacy/survey/intro.html

[10] Solove, D. J. (2010). The meaning and value of privacy appeal for a pluralistic definition of the concept of privacy. Open! Platform for Art, Culture & the Public Domain. https://onlineopen.org/the-meaning-and-value-of-privacy.

the amendments to the constitution[11], it does not provide full legal protection as it is not expressly contemplated in the Constitution of the United States.

There is a tendency to consider that personal information in online media is in danger, more than half of the citizens of the United States believe that their personal information is more insecure today than compared to five years ago[12]. The study prepared by the Pew Research Center[13] shows the little faith that United States citizens have in private or public institutions to protect their personal information. The United States has legislation regarding data protection; however, there is no central federal regulation regarding data protection, as can be seen in the European Union and the General Data Protection Regulation. It is not possible to speak of comprehensive legislation regarding the protection of data in the United States, but it is only possible to speak of a series of laws regarding data privacy that is focused on the privacy of consumers and that it emanates from the states to its residents.

There is no general framework that regulates the right to data protection in the United States as it can be found in the European Union. There is a fundamental difference between both structures, and this is that in the European Union data protection and privacy, in general, are fundamental rights in its legislation, and it is possible to enforce it, while this kind of protection cannot be found in the United States legislation.

Data protection is of utmost importance in a modernised society. All companies have information about their clients, such as personal files, product information, financial transactions, etc. The importance of this information lies in that the administrative decisions of a company are typically based on the personal data of its customers to make a more efficient and successful product. It is even possible to point out that there are companies that are dedicated to making profits through the management of personal data. Therefore, data protection should be the number one priority when regulating the legislative framework regarding data protection. In a specific case, it is possible to take the case of cell phones.

[11] Mr. Justice Black in his dissenting opinion concerning the Griswold v. Case. Connecticut challenged majority opinion by finding and applying the right to privacy in the United States Constitution. See more Stanley v Georgia; Roe v. Wade (1972).

[12] Smith, A. (2017). Americans and Cybersecurity Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives. Pew Research Center. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

[13] Ibid.

Not all people use social networks, but it is possible to point out that most of the population in the United States use a cell phone. It is possible to say that 90-91 per cent of the population of the United States has or uses a cell phone[14].

Our cell phones, even if we are not using them, leave records of the places we visit. Cell phones connect to specific antennas of your service provider company, so it is always leaving a trace of the places you are visiting. In addition, with only 4 points containing a timestamp and location taken from the data collected from a cell phone, researchers have been able to track 95% of people[15]; The applications that we have installed on our cell phones have provided researchers with the necessary knowledge to know the personal information of their users such as religion, marital status, languages, your tastes, etc.[16]; Researchers can use the data generated from your cell phone calls to define in advance and classify your contacts in relation to family, social or work[17]. The information or personal data that we deliver to the companies in exchange for the provision of the service we are doing it involuntarily since we are not aware of the amount and importance of the information that we are delivering. In the case of the United States' privacy system and the third-party doctrine[18], we will realise that for the judicial system of the United States, this information is being voluntarily delivered.

The problem with the doctrine previously mentioned is that it was thought with the technology existing in the 20th century, but the judges of the Supreme Court of the United States would never think about the technological advances that would exist in the 21st century. Today we live in a digital society in which countless companies keep our information; therefore, the implications of the third-party doctrine are gigantic. The information of our geolocation is available for the companies that provide us with communications services; our documents and media are stored in cloud services; our internet

[14] Lee, R. (2013). Cell phone ownership hits 91% of adults. Pew Research Center. https://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/

[15] de Montjoye, Y., Hidalgo, C., Verleysen, M. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Sci Rep **3,** 1376, pp 59*. https://doi.org/10.1038/srep01376

[16] Seneviratne, S., Seneviratne, A., Mohapatra, P. and Mahanti, A. (2014). Predicting user traits from a snapshot of apps installed on a smartphone. *ACM SIGMOBILE Mobile Computing and Communications Review, 18(2), pp.1-8.* http://dl.acm.org/citation.cfm?id=2636244

[17] Min, J. K., Wiese, J., Hong, J.I. and Zimmerman, J. (2013). Mining smartphone data to classify life-facets of social relationships. *ACM SIGMOBILE Mobile Computing and Communications Review, pp. 285-294.* http://dl.acm.org/citation.cfm?id=2441810

[18] United States v. Miller, 425 U.S. 435 (1976).

activities generate a profile of our behaviours and tastes; etc. The third-party doctrine is one of the main reasons why the fourth amendment protection cannot be applied in cases concerning 21st-century technologies.

The author of this thesis will later demonstrate and explain how the system of the right to privacy and the right to data protection is built in the United States and the European Union. The concept of privacy in the United States, and even more the concept of the right to privacy can be problematic in its definition since it is continuously evolved through the thinking of prevailing societies, and the development of new technologies. Technology has modernized various areas, the way we store our information has changed, and the way we communicate has also changed. In addition to this transformation, how we have interrupted or placed an exception to the privacy rules is not new, since it is possible to think that people thought that the mail should be private, but there are exceptions, such as the use of a postcard[19].

There are a growing fear and a sense of vulnerability as society advances in terms of our privacy. Technology has reached such a point that it is not possible to imagine our modern life without the devices we use every day and that they are also collecting information "necessary" for its operation. This information includes various edges such as where we are going, with what people we are interacting with, and even what our preferences are, just to name a few examples. The use and collection of this information can be used for different reasons, but the value of personal data must always be taken into account since if personal data is combined with the consequence that corporations do not have the technical material means to protect our information, we are talking about a hand grenade that can destroy people's life. The corporations have frequently shown us that they have failed to protect our most sensitive information[20], or that the government is watching us[21] through the information that we voluntarily or involuntarily decided to share. There are solutions to this problem/threat, it is possible to abandon the modern era and seek to live without the need to resort to technology, but that would be a solution for hermits. A complete solution that adapts to modern times is to seek broader protection that requires the discussion of new laws

[19] Menand, L. (2018). Why do we care so much about privacy?. The New Yorker. https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy

[20] Newman, L. H. (2017). All the Ways Equifax Epically Bungled Its Breach Response. Wired. https://www.wired.com/story/equifax-breach-response/

[21] Wired. (2014). Edward Snowden. Wired. https://www.wired.com/2014/08/edward-snowden/

that ensure our security in the digital life we lead or at least the creation of a new regulatory framework in which personal data is protected in the United States is sought.

The objective of this thesis is to analyze two of the models for data protection that exist in the world. The first model is the model that we can find in the United States in which the protection of personal data is sought through targeted regulation across sectors[22]. There are several shortcomings to this model since, as there is a regulation on the protection of personal data across sectors, which is contained in various federal and state laws, it is not possible to grant complete protection and easy understanding to natural persons. In contrast, the European Union model, which is mainly based on the General Data Protection Regulation ("GDPR") as the central norm that regulates the right to data protection in Europe, gives more substantial protection to the recipients of the norm by containing greater protections, rights and be based on a single regulation. The problem is to investigate is whether the regulation of data protection of the European model through GDPR has been able to influence the American model. Therefore, the questions that require development and research are the following:

1) The first problem to answer and to develop is to understand why the European model of data protection has had a global impact which has led countries outside the European Union to adopt similar regulations. The latest regulation issued by the European Union regarding data protection, better known as the GDPR, has achieved that one of the largest economies in Latin America has adopted a similar version of the text of the European Union and consecrated the lei geral de proteção de dados[23].
2) The second problem to develop is why the data protection system in the United States has adopted a regulation focused on industry sectors, in contrast to the European Union model that has developed a general regulation that covers the protection of data in general.
3) Finally, the existing dilemma will be answered and analyzed as to whether the model of the European Union has managed to influence in a certain way, the model imposed by the United States. In this case, the latest regulations issued by the state of California and future bills regarding data protection in the United States will be analyzed.

[22] Shawn, M. B. (2017). Data Protection in the United States: U.S. National Report. *Indiana University Robert H. McKinney School of Law Research Paper No. 2017-11*

[23] Lei Nº 13.709, (14th of August 2018). República Federativa de Brasil.

The methodology and technique used to achieve the objective and conduct the analysis of my research will be the analysis of the jurisprudence of the Supreme Court of the United States in which the Right to Privacy has been developed; In the case of the European Union, work will be done through the analysis of Article 8 of the European Convention on Human Rights ("ECHR"). Then, the Right to the Protection of Personal Data will be analyzed in both legal systems, contrasting it with the different international treaties on Human Rights. Finally, the research problem and the questions will be answered. The comparative method will be used during the development of this thesis to contrast the model of the European Union with the prevailing model in the United States.

The thesis is made up of 3 chapters. The first chapter aims to examine the Right to Privacy in both legal systems. You will realize that one of the first differences between both legal systems that in the system maintained by the United States there is no express mention of the Right to Privacy in the United States Constitution, but rather the Right to Privacy has been developed through a broad interpretation of the Amendments to the United States Constitution made by the judges of the Supreme Court during the 20th century. The prevailing system in the European Union differs mainly in being explicitly enshrined at the constitutional level.

In the second chapter of this thesis, the Right to Data Protection in the system of the United States and the European Union is analyzed using a comparative method. The impact of different international human rights treaties that indicate the existence of a Right to Data Protection and how they affect the regulatory system of both models will be analyzed. Finally, a presentation is made of Regulation (EU) 2016/679, better known as GDPR that regulates the data protection environment in the European Union.

In the third chapter of this thesis, the author of this thesis seeks to answer the question of why the European Union model in terms of data protection, specifically the GDPR has had a scope outside the European Union that has motivated others countries outside it to adopt similar regulations or to inspire their regulations on European data protection principles. In addition, it also develops why the United States model has focused on regulation across sectors or focused on specific sectors to be regulated, while the European Union model has sought a different approach in terms of protecting data, its approach is based on a general

regulation. Lastly, it will seek to determine if the European Union model has managed to influence in any way the United States model, in this case, it seeks to analyze whether the latest regulation issued by the state of California has an approach to the European model and GDPR.

Keywords: privacy, data protection, right to data protection, right to privacy, human rights

Acknowledgements:

Many people have contributed in various ways to the process and conclusion of this work. First, I want to thank my family for their unconditional support, love and understanding in every decision, project and adventure. My thanks also go to my partner and my friends who always supported me morally and sustained me during this process.

I want to especially thank my supervisor Paloma Krõõt Tupay for her advice, support and guidelines during the development of this work. Thank you very much for accepting me and for your commitment.

I would like to thank each professor at the Faculty of Law of the University of Tartu for the valuable experience provided. Lastly, I would like to thank the University of Tartu for giving me the opportunity to come to Estonia and find a home in this small but incredibly modern and digital Baltic Republic.

CHAPTER I. THE RIGHT TO PRIVACY IN THE US AND THE EU

1.1THE RIGHT TO PRIVACY IN THE UNITED STATES

The United States Constitution does not have an express reference to the right to privacy. Justice Louis Brandeis has noted that "The makers of the Constitution conferred the most comprehensive of rights and the right most valued by all civilized men—the right to be let alone."[24] However, despite the fact that the Federal Constitution does not expressly mention the right to privacy, we will realize that the construction of jurisprudence by the Supreme Court of the United States has granted protection to different ranges of values that they can be derived from the concept of the word privacy.

The Supreme Court of the United States has defined some protection in some of the amendments to the Constitution of the United States, for example in the First Amendment which indicates "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."[25] Association privacy has been recognized[26]; the right to public expression through anonymity[27]; and political privacy[28].

There are other interests protected in other Amendments of the Federal Constitution of the United States that will be developed in this chapter, but due to the limitations imposed by the judicial process and also because the Constitution of the United States only offers protection against intrusion of the government, it is necessary to develop laws that seek the protection of the privacy of the individual.

[24] Olmstead v. United States, 217 U.S. 478. (1928)
[25] U.S. Const. amend I.
[26] National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958)
[27] Talley v. California, 362 U.S. 60 (1960)
[28] Watkins v. United States, 354 U.S. 178 (1957)

1.1.1 The evolution of the right to privacy in the US.

As explained above, in the United States, the Supreme Court first recognized the Right to Privacy with the case of Griswold v. Connecticut to be developed later. Prior to this case, Justice Louis Brandeis had pointed out that the right to privacy was another way in which he promoted the right to be left alone[29]. However, the Right to Privacy has been developed in various cases belonging to the Jurisprudence of the Supreme Court of the United States, in which a range of values has been found in which they have been assigned a certain degree of protection. Therefore, before entering the Right to Data Protection in the United States and the European Union, it is necessary to understand how the concept of privacy in the United States evolved until it was recognized as a right.

1.1.1.1 Olmstead v. the United States.

Olmstead v. United States, 277 U.S. 438 (1928) occurred in 1927 and began to lay the foundations for the development of the right to privacy in the United States. This case proved to have been incredibly valuable and influential in future decisions in cases of the United States.

In the 1920s and later, there was a ban on the sale of alcoholic beverages that increased the federal government's role in the prosecution and combat of crime, and also increased the work of federal courts[30]. The increase in work in federal courts brought unexpected demands towards the federal government due to the ban, and the role of government in the daily life of citizens begins to be raised. This increase in the prosecution of criminals brought with it new methods that were used by the government to justify the demands presented to federal courts, and even to the supreme court, among them was the wiretapping of phones that provoked constitutional questions of difficult resolution[31].

Olmstead operated business of clandestine alcohol sales or better called bootlegging, which

[29] Warren, Brandeis, supra note 3.
[30] Hamm, R. F. (2010). Olmstead v. United States: The Constitutional Challenges of Prohibition Enforcement. *University at Albany, SUNY, Edited by the Federal Judicial Center for inclusion in the project Federal Trials and Great Debates in United States History, pp. 1.*
[31] Ibid.

consisted of the importation of alcoholic beverages from Canada, and was sold throughout Seattle, Washington[32]. In order to gather more evidence about Olmstead's criminal activity, federal officials decided to intervene his phone.

The problem was that the obtaining of the recordings through the intervention of Olmstead's phones was made without having asked for a warrant. Olmstead defended himself by saying that the federal police had violated the rights concerning the fourth and fifth amendments. Questions such as, did the use of evidence disclosed in wiretapped private telephone conversations, violate the recorded party's Fourth and Fifth Amendments? They are essential to realising how the United States judicial system understood the concept of privacy at that time.

The Supreme Court in a controversial decision, 5-4 pointed out that the government could use the evidence gathered in a criminal trial in a Federal Court since the telephone conversation voluntarily made by the accused, and that it was secretly heard due to his telephone intervention on the part of the government, it does not cause the accused to be a witness against himself in violation of the Fifth Amendment[33].

The evidence collected through the intervention of the telephones that were in the Olmstead office were carried out in the basement of a building with large offices, and in public streets, therefore a trespass was never committed towards the property of the accused. Therefore, obtaining these pieces of evidence does not violate the fourth amendment[34]. In this case, Chief Justice William Taft cited previous decisions concerning the fourth amendment in which he had applied to physical search and seizure[35].

Under the common law system, the admissibility of the evidence is not affected even when it has been obtained illegally[36].

---

[32] Ibid.

[33] Olmstead v United States, 277 U.S. 462.

[34] *Id*. At 466.

[35] Agnello v. United States, 269 U.S. 20 (1925); Gouled v. United States, 255 U.S. 298 (1921); Amos v. United States, 255 U.S. 313 (1921); Silverthorne Lumber Co., Inc. v. United States, 251 U.S. 385 (1920); Weeks v. United States, 232 U.S. 383 (1914); Boyd v. United States, 116 U.S. 616 (1886); Olmstead, 277 U.S. at 467.

[36] Olmstead, 277 U.S. at 467.

It is interesting to see how the Supreme Court of the United States understood the state intervention in private life in the light of the fourth amendment. However, it is vital to analyse the dissenting opinion of the judges and precisely that of Associate Justice Louis Brandeis. He pointed out that in Ex parte Jackson[37], it was argued that a sealed letter entrusted to the mail is protected by the amendments, in this sense, the mail is a public service furnished by the government. The telephone is a public service furnished by its authority. Therefore, if we refer to its essence, there is no difference between a sealed letter and a private telephone conversation[38]. The invasion of the privacy of a telephone conversation is a much superior to the invasion of a letter since when the privacy of a telephone conversation is invaded, the private life of two people is invaded, while the invasion of one sealed letter only implies the invasion of a person's privacy.

The protection of the fourth and fifth amendments did not apply. It is possible to understand that no physical intrusion was carried out at the time of the telephone intervening, but the experience should teach us to protect our freedom. Men are born free and must be alerted to repel any invasion of freedom by an evil-mind ruler. In this case, the decision should be reversed, since the telephone intervention is a crime contained in the laws of Washington[39].

The information obtained by the intervention of Olmstead's phones was made by federal officials acting on their own. The Eighteenth Amendment has not authorised anyone to violate the criminal laws of a state. No one gave the authority to these officers to intervene in these telephone lines, so these officers should assume a criminal sanction, but the government is morally responsible since it became aware of what its officers were doing[40].

The dissenting opinion of Justice Louis Brandeis implies that the founding fathers of the United States have conferred in their amendments a right to leave them alone, which is one of the rights that favours civilised men. The government should not violate the laws of the states to gather evidence that solves a case. This case shows a seed regarding the rights of citizens against illegal interventions by the Government. It is not possible to understand the illegal action of the government since it interferes in the private life of people without a just

[37] Ex parte Jackson, 96 U.S. 727 (1878).
[38] Olmstead, 277 U.S. 475.
[39] *Id.* At 479.
[40] *Id.* At 482-483.

cause, and without any rule, that enables it to do so.

1.1.1.2 Poe v. Ullman.

Poe v. Ullman, 367 U.S. 497, 81 S. Ct. 1752 (1961). The facts of the case can be synthesized in the following, Paul and Pauline Poe, was a young married couple, who live together and have no children. Pauline Poe had had three consecutive pregnancies that had ended with infants with multiple congenital abnormalities, and who had died promptly after birth, so she had decided to use contraceptive methods to prevent a fourth pregnancy. Another woman, in this case, Jane Doe, does not have any children, but she had recently been pregnant which caused her a deep state of physical discomfort, in which she had a period of 2 weeks unsettled, and a total of 9 weeks sick what it caused her a paralysis that caused her difficulties to speak, and emotional instability. Another pregnancy, in this case, would be very harmful to her, and therefore decides to seek a contraceptive method to prevent a second pregnancy that could be a threat to her life[41].

The women in both cases sought that the damage they had suffered would not occur again in the future. The form of prevention is through contraceptives, but unfortunately, during that time, Connecticut's law[42] prohibited doctors from facilitating contraceptive devices and giving information about them. Finally, the two women and their doctor decide to file a lawsuit s against the States Attorney, Ullman, claiming that the law violated their Fourteenth Amendment rights to due process.

Questions such as did the Connecticut law violate liberty protected by due process of the Fourteenth Amendment? Started to arise. The problematic of this case depended on a straightforward application of the law. The judges in the first instance dismissed the plaintiffs' lawsuit since the law was in the books, but it was not being applied during that time.

The Supreme Court when it received the case, determined that there had been no violation of the right to due process of the plaintiffs since the law only posed a threat to the plaintiffs,

[41] Poe v. Ullman, 367 U.S. 498-500 (1961).
[42] Conn. Public Acts 1879, c. 78.

but in this case, the law was not being applied[43]. Therefore, the freedom contained in the fourteenth amendment had not been violated.

The law had been in effect for almost 100 years[44], and it had never been applied. The judges decided to resolve with a sense of urgency and did not consider whether or not there was a violation of the constitution.

However, although the Supreme Court did not want to go into details about the violation or not of an amendment, for this particular case, it is necessary to pay attention to the dissenting opinion, and especially that of Justice John Marshall Harlan II. The underlying reason for the dissenting opinion is to go around the definition of the "Right to Privacy". Justice John Marshall Harlan II seeks to question the authority of the state of Connecticut whenever it intends to invade the private life of a couple.

"Here is the core of my disagreement with the present disposition. As I will develop later in this opinion, the most substantial claim which this married person press is their right to enjoy the privacy of their marital relations, free of the enquiry of the criminal law, whether it be in the prosecution of them or of a doctor whom they have consulted. And I cannot agree that their enjoyment of this privacy is not substantially impinged upon when they are told that if they use contraceptives, indeed whether they do so or not, the only thing which stands between them and being forced to render a criminal account of their marital privacy is the whim of the prosecutor"[45].

In the words of Justice John Marshall Harlan II, Connecticut law is considered to be violating the Fourteenth Amendment. It considers that a law that seeks to criminalise the use of contraceptive methods by a house couple is an intolerable and unjustifiable invasion of the invasion of privacy, something that interferes with one's personal life[46].

After the dissenting opinion of Justice John Marshall Harlan II, it is possible to understand that he has highlighted the right to privacy and with this new approach a new range of rights

[43] Poe, 367 U.S. at 510.
[44] *Id.* At 501.
[45] *Id.* At 536
[46] *Id*. At 539

for people in the United States.

1.1.1.3 Griswold v. Connecticut.

Griswold v. State of Connecticut was a court case decided by the United States Supreme Court in 1965.

The case was initially favourable to the plaintiff, which in this case is the state of Connecticut. Estelle Griswold, who was the director of the Planned Parenthood League of Connecticut, and Lee Buxton, the Medical Director of the same organisation, were sentenced as accessory perpetrators of the crime for providing couples with information about contraceptive methods, and in some cases writing a prescription for contraceptive devices for women[47].

The arrest of these people occurred in 1961, during that period, Connecticut law[48] prescribed as a crime for anyone who used a drug or device for the purpose of preventing pregnancy and prescribed a crime for anyone seeking to attend, advise, cause or order another person to do the same. Therefore, Estelle Griswold and Lee Buxton were found guilty of providing assistance with contraceptive methods and fined 100 dollars each.

In the Supreme Court ruling, the majority opinion refers to the Connecticut Law regarding birth control being unconstitutional regarding the fourth and fifth amendments that protect the individual's home and private life from government interference[49]. Marriage is something sacred and a private bond between two people that fall on one of the privacy spheres guaranteed in several provisions of the constitution, and also the sense of freedom found in the Bills of Right.

The decision, in this case, was in charge of Justice William O. Douglas. Justice Douglas's opinion, in this case, is that the Bill of Rights has specific guarantees, but they also have "penumbras"[50] that are created through the emanation of these guarantees to give an opinion and meaning. Through the first, third, fourth, fifth, ninth, and fourteenth, it is possible to

[47] Griswold v. Connecticut, 381 U.S. 479 (1965).
[48] Articles 53-32, 54-196 of The General Statutes of Connecticut (1958 rev.)
[49] Griswold, 381 U.S. 484-486.
[50] *Id*. At 483.

build this right to privacy that cannot be infringed[51].

Although there are differences in the basis of this ruling on the constitutional category of the right to privacy, it is possible to recognize that the right to privacy exists, is fundamental and also substantive.

The court understands that people should be free from any state interference that is not deemed necessary since the right to privacy is superior to that. “Would we allow the police to search the sacred precincts of marital bedrooms for tell-tale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship”[52].

1.1.1.3 Katz v. the United States.

The case is about Charles Katz, a person who specialized in betting on college basketball. His activities caught the attention of The Federal Bureau of Investigation (FBI) and therefore began to investigate his betting activities. In 1965, Katz was secretly recorded while reporting his bets to the bookmakers; the FBI was able to record the entire conversation, as they had connected a listening device to one of the telephone booths near his apartment in Los Angeles. FBI agents decided to arrest Katz and accused him of transmitting bets through the US state telephone lines, which is a crime under federal betting law[53] in the United States[54].

During Katz's trial, his lawyer argued that the telephone booth he used should be considered

[51] *Id*. At 486-493.
[52] *Id.* At 486.
[53] 18 U.S.C. § 1084. That statute provides in pertinent part:
"(a) Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined not more than $10,000 or imprisoned not more than two years, or both."
"(b) Nothing in this section shall be construed to prevent the transmission in interstate or foreign commerce of information for use in news reporting of sporting events or contests, or for the transmission of information assisting in the placing of bets or wagers on a sporting event or contest from a State where betting on that sporting event or contest is legal into a State in which such betting is legal."
[54] Katz v. United States, 389 U.S. 347 (1967)

an area constitutionally protected by the Fourth Amendment of the United States. Therefore, all recordings obtained by the FBI should be excluded as evidence of the trial, since the FBI had never requested a search warrant that allowed them to place the listening device in the telephone booth[55].

The judge rejected this argument, and therefore Charles Katz was convicted based on the recordings obtained as evidence. Finally, Katz decided to appeal this ruling and therefore addressed the Supreme Court of the United States.

The main question that we must ask ourselves in order to fully understand this case is, the Fourth Amendment gives us protection against unreasonable searches and seizures by the government and therefore imposes that the government must obtain a search warrant to do so, but It is necessary to obtain a search warrant, whenever it is intended to intercept a public telephone booth?[56]

On December 18, 1967, the Supreme Court of the United States in a 7-1 decision favourably sentenced Charles Katz that invalidated the FBI's wiretap, and therefore reversed the sentence against Katz. The ruling was drafted by Justice Potter Stewart, and a series of arguments are noted:

Listening activities by the Government of the United States, in particular, FBI agents, had violated Katz's privacy while he was using the telephone booth near his apartment, and therefore when they did this listening, they constituted a "search and seizure" in a sense reflected by the Fourth Amendment. The Supreme Court judges declare that the spaces referring to a public telephone booth cannot be considered a protected constitutional area, and also the Fourth Amendment cannot be explicitly translated as a constitutional right to the right to privacy[57]. What the fourth amendment of the United States seeks is to protect the individual freedom of people against inevitable intrusions by the Government. The judges of the Supreme Court correctly affirm that the intention given by the Fourth Amendment of the United States is protection towards people, not places in particular. Whenever a person makes a call, what they are looking for is that their conversation is not

[55] *Id*. At 349-350.
[56] Katz v. United States. (n.d.). Oyez. Retrieved April 27, 2020, from https://www.oyez.org/cases/1967/35.
[57] Katz, 389 U.S. 350.

heard; therefore, the argument on the part of the Government regarding the glass material of the telephone booth is unfounded[58].

Now, the United States Government uses the argument used in Olmstead v. United States[59] and Goldman v. United States[60] every time it is argued that the scope of the Fourth Amendment is only for tangible property, therefore, in this case, it cannot be applied, because there was never a trespass to the property, as noted in "Trespass Doctrine". It is true that the United States justice system has been deciding in this way the cases concerning the Fourth Amendment, but the judges well understand that the Fourth Amendment has the objective of protecting people, and not specifically physical places of unreasonable searches and seizures by the Government. Therefore, the activities of the Government in terms of the listeners made in the public telephone booth referring to Katz's conversations constitute a search and seizure order, as indicated in the Fourth Amendment[61].

Another of the arguments that need to be deepened is the one put forward by Justice John Marshall Harlan II. This judge in his concurring opinion indicates 3 types of arguments, the first one refers to the fact that a telephone booth (closed) is a private area just like a home[62], in which any person has a reasonable expectation of privacy that is constitutionally protected; the second refers to the fact that the electronic intrusion by the government when placing the listening device in a place that is supposed to be private may constitute a violation of the fourth amendment; and that the invasion of a constitutional area protected by the FBI is allegedly unreasonable in the absence of a search and search order[63].

To get more details, when the Supreme Court's opinion points out that the Fourth Amendment protects people and not places, Harlan points out that the reference to a place had arisen from previous decisions where there was a double requirement, the first requirement is that a person has exhibited a real and subjective expectation of privacy, and the second requirement is that society considers that expectation of privacy as reasonable[64].

---

[58] *Id.* At 352-353.
[59] Olmstead v. United States, 277 U.S. 457, 464, 466.
[60] Goldman v. United States, 316 U.S. 129, 134-136.
[61] Katz, 389 U.S. at 353.
[62] Weeks v. United States, 232 U.S. 383 (1914).
[63] Katz, 389 U.S. at 360-361.
[64] *Id.* At 361.

In this case, what we are looking to raise is that a person who has a conversation in a public place cannot have a reasonable expectation of privacy, since that conversation can be correctly heard by other people, but if a person wishes to maintain a conversation in a private place if it could be understood that there is a reasonable expectation of privacy.

1.2 The reasonable expectation of privacy.

The reasonable expectation of privacy is an elementary element of the privacy laws, and that helps determine in which places, moments and activities a person has a right to privacy.

The concept of a "reasonable expectation of privacy" brings with it a series of tests so that the reasonable expectation can be determined:

a) First, the person must demonstrate a subjective or psychological element, in which he expects his activity, places or moments to be private.
b) The second has to do with what in society is considered reasonable, that is, that the subjective expectation of the individual must be considered reasonable in society[65].

People in a society may have a reasonable expectation of privacy when they have conversations over the phone and letters. Reasonable expectations may change from society to society, for example, the previous case would only apply in the United States, but in the case of the European Union, it would be possible to understand that Instant Messaging Services are also private, and no one is monitoring them.

Now, people should not have a reasonable expectation of privacy when their actions take action in a public space or when their possessions can be seen forever. In the case of privacy in electronic media, in the United States, there would be no reasonable expectation of dialled numbers, of electronic bank records and of communications maintained through these electronic media.[66]

The cases of a reasonable expectation of privacy mentioned above can be easily solved at

[65] 68 American Jurisprudence 2d Searches and Seizures §9 (1962).
[66] 15B American Jurisprudence 2d Computers and the Internet (1962) §28.

the time of contrast. However, if we take privacy expectations to a modern environment, it is difficult to understand what is understood as public space, and what is understood by a private sphere. What the author of this thesis intends to point out is that historically the judicial system of the United States has always had to look at the fourth amendment of its constitution to find some kind of privacy protection, and it has been interpreted in different ways. The protection of privacy from the beginning could be understood as the right to leave you alone, protection of the home, freedom from government surveillance, etc. However, there is no law in the United States that seeks privacy protection nationally.

The courts of the United States continue to apply the same logic for the resolution of cases, using legal precedents that are unable to solve new cases concerning the digital world in which we live.

It is understandable that the creation of a reasonable expectation of privacy in Katz v. United States has reflected a thought of how privacy was understood in the years 1967, but the author of this thesis thinks that the lack of initiative by the United States Congress to legislate on a national law that seeks the Privacy protection of individuals, to have had to be results with the effort of the judiciary.

Later the author of this thesis will develop this idea in-depth, but first, it is necessary to delve into the idea of the third-party doctrine and how it was developed.

1.3 The third-party doctrine.

The third-party doctrine is a legal doctrine that is part of the legal system of the United States, and that in simple terms maintains that people who voluntarily decide to deliver information to third parties (whatever the service) do not have a reasonable expectation of privacy[67]. This allows the Government of the United States to obtain information from a person by going to these third parties without a legal warrant and without complying with the prohibition established in the fourth amendment of the Constitution of the United States.

[67] See Issacharoff, L.; Wirsha, K. (2016). Restoring reason to the third-party doctrine. *Minnesota Law Review, 100(3), 985-1050*; Gentithes, M. (2020). App permissions and the third-party doctrine. *Washburn Law Journal, 59(1), 35-52*; Kerr, O. S. (2009). The case for the third-party doctrine. *Michigan Law Review, 107(4), 561-602.*

The United States Fourth Amendment does not prohibit information voluntarily disclosed to a third party, and obtained by government authorities, from being used, even if the information was voluntarily disclosed in the belief that it will only be used for the purpose collected and that the trust that has been placed in that third part will not be undermined[68].

1.3.1 The United States v. Miller.

The case deals with Mitch Miller who was sentenced for running an alcohol distillery business, was caught carrying necessary equipment for the alcohol distillery, and bottles of whiskey on which the alcohol tax had not been paid[69]. The Bureau of Alcohol, Tobacco, and Firearms (ATF) issued subpoenas to two of Miller's banks asking for records of all Mitch Miller account transactions. The evidence collected by the AFT was used in the trial against Miller in which he was sentenced in the first instance, but the United States Court of Appeals reversed that ruling, stating that Miller's rights under the United States Fourth Amendment had been violated.

The case was brought to the United States Supreme Court in which the overriding question to answer was whether the records obtained from Miller's accounts constituted a violation of the Fourth Amendment. The Court held that the bank records obtained by the AFT were not under the protection of the Fourth Amendment, and therefore the District Court had not erred in its judgment in denying the motion to repress[70]. The court held:

a) That the records seized were not Miller's private papers, but records of the businesses that banks regularly use[71].
b) It is not possible to find a legitimate expectation of privacy in the content of the deposit vouchers and checks since they are commercial instruments used in commercial transactions and not confidential communication mechanisms[72]. The seized documents are information that is voluntarily transmitted to banks and their employees to naturally conduct a business[73]. The fourth amendment does not

[68] United States v. Miller, 425 U.S. 435, 443 (1976).
[69] *Id*. At 435.
[70] *Id.* At 440-446.
[71] *Id.* At 440-441.
[72] *Id.* At 441-443.
[73] *Ibid.*

prohibit the collection of information disclosed to a third party and transmitted by that third party to a government authority[74].

1.3.2 Smith v. Maryland.

This case is about installing a pen register to record the numbers dialled from Smith's home phone. This installation was made at the request of the police in order to gather information about a theft case. Smith prior to the robbery trial, asked to suppress any result from the pens because it violated his Fourth Amendment right. The Maryland court denied Smith's motion arguing that the installation of the pen register did not violate his Fourth Amendment right. Smith appealed, but the Court of Appeals upheld the judgment issued by the Maryland Court[75].

The United States Supreme Court held that the installation and use of a ballpoint pen registration did not constitute a search under the terms contained in the Fourth Amendment and therefore it was not a requirement to obtain a warrant from the police to carry out said operation[76]. The arguments were:

a) The application of Fourth Amendment protection is conditioned on whether the applicant seeking its protection can claim a legitimate expectation of privacy that has been invaded by some government authority. For this legitimate expectation of privacy to operate, two requirements must be met, the first having to do with the fact that the individual must have exhibited a subjective expectation of privacy, and the second requirement is that the subjective expectation of the subject is a reasonable expectation within a society[77].
b) In this case, Smith did not have a subjective expectation of privacy over the phone numbers he dialled, and even if he did, his expectation could not be considered legitimate. The court's argument states that phone users should have a general expectation of privacy regarding the numbers they dial as they should be transmitted

[74] *Ibid.*
[75] Smith v. Maryland, 442 U.S. 735 (1979).
[76] *Id.* At 739-746.
[77] *Id.* At 739-741; Katz v. United States, 389 U. S. 347 (1967).

> to the phone company and the phone company should have the facility to record this information, record for commercial purposes, etc.; Smith was unable to demonstrate this expectation using his home phone as he could have used a public phone. Furthermore, this subjective expectation cannot be considered reasonable within a society since Smith voluntarily transmitted the numerical information to the telephone company[78].

With the cases of United States v. Miller and Smith v. Maryland establishes the third-party doctrine which has been used countless times by the United States Courts to determine the extent of protection of the Fourth Amendment regarding privacy. This doctrine states that persons who voluntarily provide information to a third party are not protected by an expectation of privacy, and therefore government authorities can obtain information without the need for a warrant.

The development of the Third-Party doctrine during the 20th century brought with it answers to problems posed with the technology of that time. However, it was not possible for the judges of the Supreme Court of the United States to imagine the type of technology that would exist in the future, today too much data is in the hands of third parties. Recent cases of the Supreme Court such as United States v. Jones in which Justice Sonia Sotomayor points "People disclose the phone numbers that they dial or text to their cellular providers, the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers… I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[79] The Supreme Court applied reasoning similar to that of Justice Sotomayor in Riley v. California. The problem is if the government could search the content (data) of a cell phone in search of the arrest incident[80]. The third-party doctrine has remained constant throughout the decades. However, the Supreme Court has defined exceptions, for example, individuals have a reasonable expectation of privacy in luggage placed in overhead

[78] Smith, 442 U.S. at 736.
[79] United States v. Jones, 565 U.S. 417 (2012).
[80] Riley v. California - 134 S. Ct. 2473, 2480 (2014).

compartments on a bus[81]; in hotel rooms where guests stay, even when there is express permission from third parties to access their rooms[82].

The fundamental problem that lies in the third-party doctrine is that with technology as modern as it exists today, too much data is in the hands of third parties. We must think that we live in a digital age in which we store photos and documents with our cloud providers, our internet history is in the hands of ISPs, etc. It is no longer necessary for the government to enter people's homes to learn from a specific person since all the necessary data is in the hands of third parties. Furthermore, it must be remembered that part of the doctrine developed in Smith v. Maryland assumed that people were voluntarily providing that information to telephone companies. It is not possible to apply this same reason today, because it is impossible to think that people chose not to use a phone when technology is so immersed in our lives.

However, there is a tendency to rethink the third-party doctrine with the Carpenter case. In Carpenter v. Unites States, the United States Supreme Court notes that individuals have a reasonable expectation of privacy under the Fourth Amendment regarding cell towers that disclose information about the location of individuals[83]. What the Supreme Court holds in Carpenter v. United States is of vital importance since, under the third-party doctrine, an individual does not have a reasonable expectation of privacy, and therefore no protection under the Fourth Amendment, on information voluntarily disclosed to third parties. There is an essential change in the reasoning of the Supreme Court since it understands that the simple fact of using a cell phone, an individual is giving information about his location, in which this data is not being voluntarily given[84]. However, the Supreme Court expressly limits the extent of Fourth Amendment protection to CSLI, wasting an opportunity to clarify important issues regarding Fourth Amendment jurisprudence in a digital age. Courts of the first instance in the United States have refused to interpret the case of Carpenter v. United

[81] Bond v. U.S., 529 U.S. 334 (2000).
[82] Stoner v. California, 376 U.S. 483 (1964).
[83] Carpenter v. United States, No. 16-402, 585 U.S. 2215-2216 (2018).
[84] Carpenter, 201 U.S. at 2218.

States in a broad way to deal with similar problems[85]. However, in Naperville Smart Meter Awareness v. City of Naperville, No. 16-3766 (7th Cir. 2018) positive signs is given indicating that the United States Courts in the near future may build their arguments on the basis of Carpenter v. United States for reasons of extending Fourth Amendment protection to various types of personal data.

1.2 The right to privacy in the European Union.

Article number 1 of the European Charter of Human Rights indicates "Human dignity is inviolable. It must be respected and protected.[86]" In the European Union, human dignity is recognized as an absolute fundamental right. The right to privacy or to live a private life is enshrined in article 12 of the Universal Declaration of Human Rights, in article 7 of the European Charter of Fundamental Rights (EU Charter) and in article 8 of the European Convention of Human Rights (ECHR).

Article 8 of the European Convention on Human rights enshrines the right to privacy in the European Union. The scope of application of this article falls on 4 identified interests, a) private life; b) family life; c) home and d) correspondence. The second part of the article has to do with determining if there has been an interference not permitted by law in one of the interests mentioned above, or if the state has a positive obligation to protect the right to privacy[87].

The European Court of Human Rights has developed the scope of Article 8 ECHR through its jurisprudence, in which there is no definition of private life[88], and the term of private life is broad[89]. Furthermore, its jurisprudence regarding files or data collected by security

[85] Cheng, R. (2018). Say the Secret Word: Court Allows Cellphone Search Despite Password Request before Miranda Warning. Forbes. https://www.forbes.com/sites/roncheng/2018/08/09/say-the-secret-word-court-allows-cellphone-search-despite-password-request-before-miranda-warning/#2b2d18af771d

[86] Council of Europe., & Council of Europe. (2000). The Charter of Fundamental Rights of the European Union. Art. 1.

[87] European Court of Human Rights. (2019). Guide on Article 8 of the European Convention on Human Rights, Right to respect for private and family life, home and correspondence. https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf. Pp. 7.

[88] ECtHR 13710/88, Niemietz v. Germany.

[89] ECtHR 44647/98, Peck v. The United Kingdom.

services or the state is quite extensive[90].

The ECHR was born as a product of the consequences of the Second World War[91] and had a direct relationship with the Universal Declaration of Human Rights[92]. Article 8 ECHR was drafted in a negative way to promote freedom and prevent illegal interference by states. However, through the practice of the European Court of Human Rights (ECtHR), Article 8 ECHR has been interpreted as a right stemming from the personality of the individual, promoting the liberties of individuals and forcing states to adopt positive measures to protect this right. In the words of van der Sloot, the practice of ECtHR has led to a considerable expansion of the scope of the right to privacy[93].

A) The right to privacy has been used by ECtHR to grant protection in different matters that mainly fall on other rights and freedoms contained in the ECHR, such as the right to marriage, the right to a fair trial, and the protection of the reputation of people[94].
B) The right to privacy has come to replace the absence of other rights and freedoms such as development to develop personality, the right to property, the right to residence, and legal identity[95].
C) Article 8 ECHR has been the main argument under which the ECtHR has built its jurisprudence and has opened the ECHR to new rights and freedoms, such as the right to data protection, minority rights, and the right to clean and healthy environment[96].

As for the recognition of the right to data protection, there is no problem, since it is possible to refer to article 8 EU Charter. Furthermore, the right to privacy, together with the right to

[90] ECtHR 33810/07, Association "21 December 1989" and Others v. Romania; ECtHR 27798/95, Amann v. Switzerland; ECtHR 9248/81, Leander v Sweden; ECtHR 7215/75, X v. United Kingdom; ECtHR 74336/01, Beteiligungen GmbH v. Austria.
[91] Weil, G. L, & Goodrich, L. M. (1963). The European convention on human rights: background, development and prospects. *Leyden: Sythoff.*
[92] United Nations, supra note 8, preamble.
[93] van der Sloot, B., (2015). Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data". *Utrecht Journal of International and European Law, 31(80), pp.25–50.*
[94] *Id*. Chapter 2.
[95] *Id.* Chapter 3.
[96] *Id.* Chapter 4.

data protection, are dealt with in different articles in the EU Charter. Therefore, it is possible to argue that based on the EU Charter Right to Privacy and Right to Data Protection are independent each other. Finally, the right to privacy is enshrined in both Article 8 ECHR and Article 7 EU Charter.

Regarding the right to data protection enshrined in Article 8 EU Charter maintains that all people have the right to the protection of their personal data and that the processing of that data must be fair and with specific purposes based on consent. of the person or other legitimate basis prescribed by law. It also maintains that this right guarantee access to said data that has been collected regarding him and they have the right to be rectified[97]. The right to data protection in Europe is protected by articles 8 EU Charter, article 8 ECHR, the regulation (EU) 2016/679, better known as the General Data Protection Regulation.

[97] *Ibid.*

CHAPTER II. THE RIGHT TO DATA PROTECTION IN THE US AND EU

It is possible to understand that there is no legislation concerning the protection of data in the United States, but many laws that have been drawn up both at the federal and state levels. Besides, this right is not widely developed in the laws when compared to the European Union[98].

The United States lacks a comprehensive and straightforward regulatory framework in which both citizens and companies understand the regulation of the collection and in addition to the use of this personal data. The United States Congress every time it has tried to regulate the protection of data has only regulated specific sectors, such as data concerning the health or privacy of children, but has not created single legislation regarding the protection of personal data that are intended to protect the privacy of United States citizens, and that put an end to the problem between state and federal laws regarding data protection.

2.1 The right to data protection derived from the right to privacy.

The right to privacy in the United States has been discussed on countless occasions, but it is possible to point out that the Right to Privacy as such began to be discussed after the publication of the article[99] written by Samuel Warren and Louis Brandeis in which it is discussed the Right to Privacy as a "right to be let alone". After this event, the recognition of this right has evolved from the problems that may arise from the private sphere of people to the problems that may arise in much more contemporary society. Other authors point out that after reviewing various cases of the right to privacy in the United States and the definitions proposed by the academies, the right to privacy could be defined as:

“The right to privacy is our right to keep a domain around us, which includes all those things that are parts of us, such as our body, home, thoughts, feelings, secrets and identity. The

[98] Frontier Technology. (2015). The differences between EU and US data laws. Frontier Technology. https://www.frontiertechnology.co.uk/differences-between-eu-and-us-data-laws/

[99] Warren, Brandeis, supra note 3.

right to privacy enables us to choose which parts in this domain can be accessed by others, and control the extent, manner and timing of the use of those parts we choose to disclose."[100]

In this definition of the Right to Privacy, it is already possible to find nuances that have reference to a Right to Data Protection, in which the subjects of law have the right to control what type of personal information can be accessed by other people, to have control of what type of information is shared with other people, and to what extent this information is shared. The social and historical framework in which the society of the United States and the entire world is extremely different from what Warren and Brandeis could have imagined. Social relations between people are subject to a type of communication and information exchange in which everything depends on technology. Technology is continuously developing, and society today is part of one of transmission of data and information that generates a constant threat to people's private lives. The law must be at the service of social changes, and mainly on how technology affects our lives. Laws have encountered several difficulties in protecting people's private lives since there is always a duality between protecting people's private lives and disclosing personal information to third parties.

Another perspective is suggested by the authors Tessaro and Trojani, in which they suggest that there is a deep connection between the concepts of freedom, equality, democracy, dignity and privacy in which the concept of the Right to Privacy cannot be considered as a "right to be left alone."[101] In this case, we see ourselves in a process in which the transition from the understanding of the initial concept of the Right to Privacy as a "right to be left alone" has changed to a right in which people are in control of their personal data, and also has influenced the procedures of the subjects that operate with this data. The society of the United States and the world has evolved, and with it, the right to privacy has also done so. The right to privacy has evolved to such an extent that it is considered as part of a fundamental right for subjects who belong to a society. Therefore, today there are new risks associated with the concentration of personal information in the hands of public or private institutions in which the risk to be disclosed is high, which is why the right to personal data protection derives from the right to privacy.

[100] Onn, supra note 7.

[101] Tessaro T., Trojani F. (2006), Privacy e accesso ai documenti nell'Ente locale. *Maggioli Editore p. 56.*

There is no definition of its own in the legislation of the United States that indicates what is understood by the right to personal data protection; however, the European Union Charter of Fundamental Right in its article 8 indicates:

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."[102]

The right to data protection is possible to define it as a right designed to protect a person's personal information, the right grants self-determination to the person in whom the subject of rights is informed and has the right to decide what type of personal information is willing to share with others. This right is of the utmost importance as it seeks to protect the rights and freedoms of the subject of rights from possible discrimination based on their religious beliefs, their opinions, their health, etc.

The European case differs entirely from the United States case. In the United States Constitution, there is no explicit reference to privacy or data protection, while in the European case, there is an explicit mention at a constitutional level. Article 8 ECHR is quite similar to Article 7 EU Charter, which indicates the right to respect for privacy, family life, home and communications[103].

In the case of the right to data protection, this is contained in article 8 EU Charter, but there is no express mention in the ECHR that falls under the jurisdiction of ECtHR. However, the ECtHR has extended the scope of Article 8 ECHR to data protection matters to give rise to a right to data protection[104]. Although privacy and the protection of personal data are closely

[102] Council of Europe., & Council of Europe. (2000). The Charter of Fundamental Rights of the European Union. Article 8.
[103] CJEU Case 136/79, National Panasonic (UK) Limited v. Commission of the European Communities. paras 17 et seq.
[104] ECtHR 27798/95, Amann v Switzerland; ECtHR 28341/95, Rotaru v Romania.

linked in ECtHR jurisprudence, they should not be treated as identical, since they are two completely independent rights. It is true that both rights may coincide in the scope of different areas, but as far as personal data processing is concerned in a fair way, or data processing with a defined purpose, it is possible to find that these rights are separated.

2.2 The right to data protection as a crucial human right.

There are various human rights treaties in which a Right to Privacy is proclaimed, and it is even possible to find treaties in which the Right to Data Protection would be implicit. The protection of the Right to Privacy and its promotion can be found in various international treaties such as:

- Article 17 International Covenant on Civil and Political Rights ("ICCPR");
- Article 12 Universal Declaration on Human Rights ("UDHR");
- Article 14 International Convention on the Protection of All Migrant Workers and Members of Their Families ("ICRMW");
- Article 16 Convention on the Rights of the Child ("CRC");
- Article 8 European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR");
- Article 11 American Convention on Human Rights ("ACHR")

If the reader of this thesis takes special consideration in each of these articles, it will be possible to understand that the rights and freedoms enshrined in these international human rights treaties are the inspirational principles behind the laws in relation to data protection. In this case, the author of this essay wants to thoroughly analyze the art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), art.17 of the International Covenant on Civil and Political Rights (ICCPR), and art. 11 of the American Convention of Human Rights (ACHR)

Article 17 of ICCPR provides:

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks."[105]

Article 11 of ACHR provides:

"1. Everyone has the right to have his honour respected and his dignity recognized.

2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation.

3. Everyone has the right to the protection of the law against such interference or attacks."[106]

Article 8 of ECHR provides:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary for a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[107]

All the aforementioned provisions are written in a way that implies a prohibition of interference with people's private life, and this interference could be public or private[108]. In addition, there is a respect for private life, but it is clear to point out that the fundamental principles of data protection can be found in international treaties concerning Human Rights,

[105] United Nations General Assembly. (1966). International Covenant on Civil and Political Rights. *vol. 999, p. 171* article 17.
[106] Organization of American States (OAS). (1969). American Convention on Human Rights, "Pact of San Jose". Article 11.
[107] Council of Europe., & Council of Europe. (1952). The European convention on human rights. Strasbourg: Directorate of Information. Article 8.
[108] Bygrave L. (2010). Privacy and Data Protection in an International Perspective. *Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010. Pp 181*

but especially Article 8 of ECHR, Article 17 of ICCPR and the Article 11 of ACHR would have key provisions to understand the rationale behind the Right to Data Protection

2.2.1 Article 11 of the American Convention of Human Rights.

Article 11 of ACHR establishes the Right to Privacy in a manner very similar to that established in Article 12 of the UDHR:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Article 11 of ACHR stipulates protection of the Right to Private Life and also a protection towards the individual of any unlawful attack on its honour or reputation. It is possible to determine that in this article the fundamental principles of data protection are found, but at the level of application to cases, the Inter-American Court of Human Rights (IACtHR) has not sufficiently developed the scope of ACHR so that the concept of protection of Data is fully incorporated. The decisions of the IACtHR in the matter of Article 11 have been concentrated as regards the Right to Privacy, but only based on a violation of privacy through a physical intrusion, as were the decisions of the European Court of Human Rights (ECtHR) in its first decisions regarding the right to privacy[109]. Therefore, the IACtHR has not made a broad interpretation of the Right to Privacy in relation to the protection of data; instead, its failures have embraced the Right to Privacy in a traditional way of interpretation, through physical intrusion to people's privacy[110].

Article 11 of ACHR has not been developed based on cases by the IACtHR; therefore, it has not been possible to develop the Right to Data Protection based on this article. On the other hand, the cases developed based on article 17 of ICCPR and article 8 of ECHR have had this development and construction, in addition to requiring the implementation of the basic principles related to data protection, therefore article 17 of ICCPR and article 8 of ECHR

[109] Bygrave, L. (2002). Data Protection Law: Approaching its Rationale, Logic and Limits (Information Law Series Set). *Kluwer Law International. Ch 7.*

[110] IACtHR Judgment of July 6, 2009, Escher et al.v. Brazil.

can be considered as instruments with the objective of protecting the data, while article 11 of ACHR not having this development by the IACtHR cannot have this consideration[111].

As there is no development by IACtHR, most South American countries have had to promote data protection mechanisms through the *habeas data* concept. This concept derives from the law and is a jurisdictional action that is formally enshrined in the constitution of some countries[112], and that confirms the existence of the right to any natural or legal person to request and obtain the present information about their person, and to request its elimination or correction if it were false, incorrect or simply outdated. The regulatory framework in Latin America is quite precarious as it only concentrates data protection depending on the concept of habeas data. However, it is possible to see a change of perspective in some Latin American states such as Uruguay and Argentina in which they have requested the evaluation of their legislation regarding the Convention for the protection of individuals with regard to automatic processing of personal data to the European Union[113]. Although most Latin American countries are actively participating in the global transformation in terms of technology, and are adapting their regulations based on new advances in technology, it is not possible to point out that there is adequate data protection since less than half of the Organization of American States has implemented an adequate system of data protection[114].

The IACtHR has served as an instrument in the creation of an appropriate atmosphere in which the South American states have been informed of the problems related to data protection. Moreover, the Inter-American Court of Human Rights has written guidelines related to the abusive behaviours that private actors can make regarding personal data of

[111] Bygrave, supra note 109 at 181.
[112] In Colombia through the Constitutional Court, Law 1266 of 2008, Law 1273 of 2009, Law 1581 of 2012; In Uruguay through its Constitution, Law 18.831 of 2008, Decree 232/010.
[113] Organization of American States (OAS). (1969). American Convention on Human Rights, "Pact of San Jose". Article 23.
[114] DLA Piper's Data Protection, Privacy & Security group. (2014). Data Protection Laws of the World Handbook. Available at https://www.dlapiperdataprotection.com/

individuals, and also advising states not to arbitrarily interfere in the data it contains. personal information[115].

2.2.2 Article 17 of the International Covenant on Civil and Political Rights.

The analysis of Article 17 of ICCPR is particularly significant since ICCPR is one of the treaties concerning Human Rights with the most extended reach, being ratified by more than two-thirds of the countries worldwide[116]. The cases developed based on Article 17, ICCPR provides the most unambiguous advances and indicators of the right to privacy in an international framework that enshrines the main principles related to data protection.

"As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. Accordingly, the Committee recommends that States should indicate in their reports the laws and regulations that govern authorized interferences with private life."[117]

"The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures must be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in electronic data files, and for what purposes. Every individual should also be able to

[115] Canton, S. (2002). The Role of the OAS Special Rapporteur for Freedom of Expression in Promoting Democracy in the Americas. *56 U. MIAMI L. REV. 307, 309 pp 312-13.*

[116] United Nations General Assembly. (1966). International Covenant on Civil and Political Rights. *vol. 999, p. 171.*

[117] United Nations Human Rights Committee (HRC). (1988) CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. Para 7.

ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."[118]

At the 35th International Conference of Data Protection and Privacy Commissioners Privacy: A compass in turbulent World argued that there is international pressure for the creation of binding international agreements regarding data protection to safeguard Human Rights by protecting the privacy, the personal data and the integrity of the networks in which the transparency of the data processing is increased[119]. This conference resolved to call on all governments to defend the adoption of an additional protocol Article 17 of ICCPR, which should be based on the standards that have already been developed and enshrined by other international conferences and the provision of General Comment No. 16 of ICCPR in order to create a global standard applicable to data protection and privacy protection according to law[120].

Article 17 of ICCPR adopted by the General Assembly of the United Nations in 1966 and ratified by 173 states[121] provides a legal framework for privacy protection. However, it is not possible to point out that Article 17 of ICCPR and general comment number 16 of the UN Human Rights Committee give an account of extensive protection of the right to data protection. In general comment number 16 there is no reference to the fact that special categories of personal data should need an exceptional level of protection and much harder[122]; Nor is reference made to the fact that personal data collection should be done in a fair manner; nor does it mention that personal data stored must ensure that it is not accessed by unauthorized personnel.

---

[118] *Id* at para 10.

[119] Resolution on anchoring data protection and the protection of privacy in international law. 35th International Conference of Data Protection and Privacy Commissioners Privacy: A compass in turbulent world. Warsaw, 23-26 September 2013.

[120] Ibid.

[121] United Nations Human Rights Office of the High Commissioner. Status of Ratification. Ratification of 18 International Human Rights Treaties. Available at https://indicators.ohchr.org/.

[122] Special categories of personal data or sensitive personal data refers to the fact that there are certain types of personal data that due to their sensitivity, better protection measures should be granted to ensure their protection. Among the special categories of data it is possible to find, racial or ethnic origin, political opinions religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sex life and sexual orientation, generic data and biometric data.

The United States ratified ICCPR in 1992[123]. The United States made 5 reservations to ICCPR, which referred to hate speech, capital punishment, the use of "cruel, inhuman, or degrading treatment" and the separation of juvenile and adult offenders [124]. Finally, the Senate added that ICCPR would not be self-executing meaning that it would not act as binding law for the courts of the United States[125]. The Senate clarified the foregoing and noted that the ICCPR would not create private causes of action in the United States Courts[126]. This brought criticism from the UN Human Rights Committee pointing out "Such treaties, and the Covenant specifically, is not a web of inter-State exchanges of mutual obligations. They concern the endowment of individuals with rights."[127]

2.2.3 Article 8 of the European Convention on Human Rights.

The article of the European Convention on Human Rights has a relatively broad scope in terms of data protection[128]. The development of data protection based on Article 8 ECHR has been made based on a case-by-case dynamic, the guarantees that have been found in regard to data protection have been related to the particular circumstances of the cases, and therefore its general application is difficult. When analyzing the purpose of article 8, it is possible to point out that the primary purpose of this article is to protect the subjects of law from any arbitrary interference against privacy, family life, home and correspondence made by a public authority[129]. "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary for a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or

[123] Thompson, A. (2008). The United States and the ICCPR. *SAIS Review of International Affairs 28(2). pp 105-106*.
[124] Ibid.
[125] Ibid.
[126] Senate Executive Report. (1992) No. 102-23
[127] Wippman, D., Dunoff, J. L., & Ratner, S. R. (2006). International Law: Norms, Actors, Process: A Problem-oriented Approach. *(2nd Edition ed.) Aspen Publishers. Pp. 437*
[128] ECtHR 9248/81, Leander v. Sweden, §48; ECtHR 27798/95, Amann v. Switzerland, §65; ECtHR 931/13, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, §§133-138; ECtHR 57375/08, P. and S. v. Poland, §130.
[129] ECtHR 588/13, Libert v. France, §§ 40-42.

morals, or for the protection of the rights and freedoms of others."[130] The definition presented above is the traditional way of presenting a right, as a negative right, and is an essential part of the right as demonstrated in Kroon and Others v. the Netherlands $31. However, this right also ensures a positive right, in which even private parties must respect each other's privacy[131].

The court has interpreted Article 8 ECHR considering that this article has two types of obligations, one positive and one negative. The negative obligation has to do with what the author of this thesis has previously indicated; mainly, the public authorities must refrain from interfering with the exercise of this right[132]. However, states must also have an active role in promoting this right (a positive obligation) in this sense there must be a positive obligation that is effective when respecting private life, these obligations may be involved with making designated measures with the objective of ensuring respect for private life even in the sphere of relations between private parties[133]. What is logical is that with a positive obligation, a state can impose a particular behavior through given legislation not only to authorities but also to private actors.

As for the right to data protection, Article 8 ECHR began to develop with Leander v. Sweden[134]. In this case, it is analyzed if the collection and retention of personal data by the state in secret files can be used for employment vetting purposes; if a subject of rights has the right to access these files under the argument of articles 8 or 10 ECHR; and if remedial procedures and safeguards were necessary to protect against abuse of state power. In this case, it is noted that the storage of the data referring to a person's private life falls within the meaning of article 8[135]. It is now understood that the storage of the data falls on the definition of Article 8 ECHR, but now it is necessary to understand what type of data is referred to with private life. In Amann v. Switzerland notes that private life comprises two things, the

[130] Council of Europe., & Council of Europe. (1952). The European convention on human rights. Strasbourg: Directorate of Information. Article 8.2
[131] ECtHR 61496/08, Bărbulescu v. Romania, §§ 108-111.
[132] ECtHR 28341/95, Rotaru v Romania.
[133] ECtHR 5786/08, Söderman v. Sweden.
[134] ECtHR 9248/81, Leander v Sweden.
[135] Id. at §48.

first has to do with the right to live a private life, far from unwanted attention, and second the right to establish and develop relationships with other human beings[136].

Now as for the personal data that is already in the public domain, in Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, a case in which a publication of information about individuals' taxable incomes and assets in a journal. Given the circumstances of the case, the right to privacy that is contained in art 8 ECHR, the court has repeatedly stated that the concept of private life is a broad concept that is not susceptible to an exhaustive definition. Therefore, the fact that the information is already in the public domain does not necessarily mean that the protection granted in article 8 disappears[137]. "Where there has been a compilation of data on a particular individual, processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise.[138]"

Article 8 ECHR has been extensively developed by the European Court of Human Rights in Strasbourg, which contains the right to privacy but has given rise to a right to data protection too[139]. There are other international treaties such as Article 8 of The Charter of Fundamental Rights of the European Union that indicates the existence of the right to personal data protection explicitly, but since there is no express recognition of the right to data protection in ECHR, the Strasbourg court has had to develop this right through an extensive interpretation of the right to privacy. The concept of private life cannot be interpreted restrictively since the concept of privacy cannot be encompassed through an exhaustive definition. The Court of Justice of the European Union located in Luxembourg has interpreted the jurisprudence by the European Court of Human Rights regarding the concept

[136] ECtHR 27798/95, Amann v. Switzerland, §65.

[137] See more in ECtHR 40660/08 and 60641/08, Von Hannover v. Germany. The case is about taking a picture of a known character in a public place. The court noted that the publication of those photographs must be compared with the interest in privacy that person has, even knowing that the fact of appearing in public can be assimilated as public information.

[138] ECtHR 931/13, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, §136

[139] See more in ECtHR 27798/95, Amann v Switzerland, para. 65; ECtHR 28341/95, Rotaru v Romania, para 43.

of private life, the protection of personal data would be found in this concept, and would be defined as any information that made it identifiable or served to identify a person[140].

There is a clear distinction regarding the right to data protection when comparing the European Union and the United States. In the European Union, there is an explicit recognition of the right to privacy and the right to data protection, established at a constitutional level, and at the same time in the European Convention on Human Rights and the Carter of Fundamental Rights of the European Union. However, it is not possible to find such protection in the constitution of the United States since there is no express mention of the right to privacy or the right to data protection.

2.3 The right to data protection in the US legal system.

The United States does not have a unified legislative regulation in terms of data protection but instead follows a sectoral model in terms of its protection. There is no federal or national legislation that seeks privacy protection or personal data protection. On the other hand, in Europe, it is possible to find another type of approach since there is an exhaustive regulation regarding data protection[141]. The United States is primarily dependent on a combination of federal, state and a series of self-regulatory guidelines for specific industries to ensure the protection of the data of residents of the United States.

The privacy protection system in the United States is guaranteed through various instruments and case law, and they are also applied only to various industries in the United States[142]. When comparing this type of regulation with the regulation contained within the European system, at first sight, it would be possible to argue that the European regulation provides a much more robust data protection system than the United States data protection system.

[140] CJEU, Joined Cases C–92/09 and C–93/09 Volker und Markus Schecke and ECR I-11063, Eifter, para. 52.
[141] European Parliament and of the Council of Europe. (2016). Regulation (EU) 2016/679 n the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[142] See more in Public Law 104–191, "Health Insurance Portability and Accountability Act of 1996"; 20 U.S. Code § 1232g, "Family educational and privacy rights"; 5 U.S.C. § 552a, "Records maintained on individuals"; Public Law 107-347, "The Federal Information Security Management Act of 2002".

However, authors such as Swire and Kennedy-Mayo[143] point out that the data protection system in the United States is more stringent than Europe's protection system in 8 ways:

"(1) oversight of searches by independent judicial officers; (2) probable cause of a crime as a relatively strict requirement for both physical and digital searches; (3) even stricter requirements for government use of telephone wiretaps and other realtime interception; (4) the exclusionary rule, preventing prosecutors' use of evidence that was illegally obtained, is supplemented by civil suits; (5) other legal standards that are relatively strict for government access in many non-search situations, such as the judge-supervised "reasonable and articulable suspicion" standard under ECPA; (6) transparency requirements, such as notice to the service provider of the legal basis for a request; (7) lack of data retention requirements for Internet communications; and (8) lack of limits on the use of secure encryption.[144]"

Data protection as such is possible to find in the United States since 1970 with the promulgation of Fair Credit Reporting Act (FCRA)[145]. It is federal government legislation enacted with the objective of promoting justice, privacy and the accuracy of consumer information contained in the archives of consumer reporter agencies. It aims to impose limits on data that can be shared according to the consumer credit report industry, and mainly to allow an easy way for consumers to rectify errors in their reports[146]. In 1974, the United States Privacy Act was enacted[147], a federal law that establishes a code of conduct regarding the practice of fair information that the United States government collects, maintains, uses and disseminates personally identifiable information (PII) about individuals and that is kept in the system of records of federal agencies. The new act declares that the right to privacy is a personal and fundamental right protected by the United States Constitution[148].

If the data protection system of the United States is compared with the data protection system of Europe, it is possible to point out that the European system is the role model for the

[143] Swire, P., Kennedy-Mayo, D. (2016). How Both the EU and the U.S. Are 'Stricter' Than Each Other for the Privacy of Government Requests for Information. *66 Emory Law Journal 617 (2016).*
[144] *Id.* At 642
[145] 15 U.S.C. § 1681, "Congressional findings and statement of purpose".
[146] Id.
[147] 5 U.S.C. § 552a, "Records maintained on individuals"
[148] Raul, A., Manoranjan. T., Mohan, V. (2015). THE PRIVACY, DATA PROTECTION, AND CYBERSECURITY LAW REVIEW. *Law Business Research Ltd, London. pp 268-269.*

protection of the data of individuals, while the approach that has been taken in the United States is aimed at protecting consumers[149]. In the United States, at the federal level is the Federal Trade Commission (FTC) empowered through the Federal Trade Commission Act (FTCA)[150], the agency responsible for bringing the application of actions that are intended to protect consumers from unfair practices by the industry and the application is of federal regulations regarding privacy and data protection. The Privacy Act in the United States is a breakthrough in terms of Congress's commitment to the right to privacy and the right to data protection, however, to this day the United States lacks a comprehensive system.

2.4 The right to data protection in the European Union.

The right to data protection is explicitly enshrined in the treaties of the European Union and in the Charter of Fundamental Rights of the European Union (EU Charter).

"Article 8. Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or ger.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority."[151]

It is also possible to find an express mention of the right to data protection in article 16 of the Treaty on the Functioning of the European Union (TFEU).

"Article 16.

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individual

[149] McGeveran, W. (2016). Friending the Privacy Regulators. *58 ARIz. L. REV. 959. Pp 961.*
[150] 15 U.S. Code § 41. "Federal Trade Commission established; membership; vacancies; seal".
[151] Council of Europe., & Council of Europe. (2000). The Charter of Fundamental Rights of the European Union. Article 8.

with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."[152]

One of the fundamental differences between the EU Charter and other treaties on Human Rights is that the EU Charter treats the Data Protection Law as an independent right, while the other treaties treat the Right to Data Protection as a derivation of the Right to Privacy[153]. However, there are certain peculiarities regarding the proclamation of this right to data protection, since it is possible to go back to 1995 when Europe promulgated the European Data Protection Directive[154], but no reference was made to the Right to Data Protection. Everything points to the fact that the Right to Data Protection was proclaimed based on Article 286 EC, The Data Protection Directive, Article 8 ECHR and Convention number 108 of the Council of Europe[155].

There are theories as to why the Right to Data Protection was introduced as a separate right to the Right to Privacy in the EU Charter. The authors Rouvroy and Poullet consider that the reason why the right to data protection was included in the EU Charter was for the purpose of extending the protection of the set of data protection rules to areas where there had not been covered by the Data Protection Directive[156]. This seems to be a correct consideration since it is possible to extend the scope of protection of a norm through the express recognition of a fundamental right. The entry into force of the Lisbon Treaty[157] in 2009 brought with it the configuration of the Right to Data Protection as an autonomous right.

The elevation of personal data protection to a category of Fundamental Rights of the

[152] European Union. (2007). the Treaty on the Functioning of the European Union. Article 16.
[153] Lynskey, O. (2014). Deconstructing data protection: The added-value of right to data protection in the EU legal order. *International and Comparative Law Quarterly, 63(3). Pp 570.*
[154] European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
[155] Lynskey, supra note 153.
[156] Rouvroy A., Poullet Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. *In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht.*
[157] European Union. (2007). the Treaty on the Functioning of the European Union. Article 16.

European Union brings with it an important decision by the legislator to reinforce the adequate protection of personal data of individuals in the European Union. However, prior to the implementation of the Lisbon Treaty, European Union legislation based its protection of personal data on fundamental rights and freedoms of individuals, and above all on Article 8 of the European Convention on Human Rights[158]. In addition to article 8 ECHR, we find the Data Protection directive adopted in 1995 that comes to protect the fundamental rights, freedoms and privacy of individuals in relation to personal data processing[159].

With the Lisbon Treaty, the form of protection of the Fundamental Rights of the European Union was redefined, granting that the European Charter of Human Rights has the same value as the treaties of the European Union. This brought with it the development and improvement of the Charter's legal status, but also uncertainties regarding the role the Charter plays in relation to other sources of fundamental rights protections relevant to the legal system of the European Union, and the interpretation of the new protective architecture of the European Union[160].

Apart from the EU Charter and other international treaties, it is possible to find regulation focused on the digital age. In the European Union, there is Regulation 2016/679[161] focused on the protection of natural persons regarding the processing of their personal data, and the transfers of personal data. On May 25, 2018, the 2016/679 regulation, better known as the General Data Protection Regulation, came into effect. The new regulation brought with it a series of modifications regarding the processing of personal data and also replacement of the old Data Protection Directive 65/46/EC. GDPR is a regulation that is thinking about the regulation of privacy in a digital age, in which people will have the option to grant permission to companies to use their data.

[158] Council of Europe., & Council of Europe. (2000). The Charter of Fundamental Rights of the European Union.

[159] European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Article 1. (1), Article 1 (2).

[160] González, G., Gellert, R. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers & Technology, 26:1. Pp 73-82*

[161] European Parliament and of the Council of Europe. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The most notable changes it brought with it were:

A) "The fines imposed under the GDPR law ranges up to 20 million Euros or 4% (four per cent) of the company's annual turnover;
B) The actions initiated against the violators and the compensation awarded to the victims of a data breach;
C) The control over personal data; and
D) The expanded jurisdiction of the law even on the companies incorporated outside the EU and doing business with companies inside the EU.[162]"

The fundamental difference between the old data protection law in the European Union and the GDPR is that the old law only regulated institutions that were within Europe and its member states, but the GDPR also affects companies that are incorporated outside of Europe, therefore represents a radical change in the game scheme. This brought with it a new way in which data processing should be handled outside of the European Union. The subjects that are bound by GDPR will have to evaluate the risks that the processing of the data supposes and, in the cases, that there is a higher risk they will have to prepare data protection impact assessments (DPIAs)[163]. They will have to implement systems that are capable of responding to all requests that arise based on the rights conferred by GDPR on its users[164]. and many more other requirements that have the objective of returning control to individuals over their personal data and simplifying the regulatory environment for international business[165]. This means that companies established in countries with more flexible data protection regulations will have to educate themselves and adopt more rigorous mechanisms to protect personal data in order to comply with the requirements imposed by GDPR.

In a particular case, companies that are established in the United States will have to approach the protection of personal data in a different way if it is personal data from the European

[162] Ganotra, S. (2018). Gdpr compliant or not. *Court Uncourt | STA Law Firm: Volume V Issue VI. pp 2-4.*
[163] European Parliament and of the Council of Europe. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Article 35.
[164] Id at Article 15-20.
[165] Council of the European Union. (2015). 9565/15, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Available at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

Union. The expansive effect that GDPR has and that reaches companies in the United States makes us rethink the protection granted by the American legislation, and therefore look for other protection mechanisms to guarantee more excellent protection to individuals residing in the United States.

CHAPTER III. EU INFLUENCE ON DATA PROTECTION IN THE US MODEL

3.1 Why the European Union model has influenced the international scene.

The model of the European Union, which is characterized by providing a complete set of rules ready to regulate and protect personal data and also grant and guarantee rights of action to its holders. The European Union model seems to be suitable in the sense that regulation (EU) 2016/679 seeks the protection of natural persons regarding the processing of their personal data and the free movement of that data. Furthermore, regulation is seen as a fundamental step in strengthening the fundamental rights of individuals in a globalized, digital society and that facilitates business activity by clarifying the rules to create a unique digital market[166].

Some laws worldwide have implemented a similar approach to that regulated by the General Data Protection Regulation[167]. Legislation around the world is seeking to resemble the European model, but it is necessary to ask why the European model is considered the standard to follow. There is no doubt that there is a primary need for regulating the protection of personal data at the international level. The attempts so far have been the Convention 108[168] established by the Council of Europe and the Privacy Guidelines[169] issued by the Organization for Economic Cooperation and Development (OECD).

The document issued in 1980[170] and then updated in 2013[171] sets out the basic principles that national legislation should have such as a) Collection Limitation Principle; b) Data

[166] European Commission. Data protection in the EU. European Commission. Available at https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[167] See Lei Nº 13.709, (14th of August 2018). República Federativa de Brasil, that unifies more than 40 different regulations regarding personal data protection both online and offline.

[168] Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe Treaty Series 108. Strasbourg: Council of Europe.

[169] Organization for Economic Cooperation and Development. (2013). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.

[170] Ibid.

[171] Organization for Economic Cooperation and Development. OECD work on privacy. OECD. Available at http://www.oecd.org/sti/ieconomy/privacy.htm.

Quality Principle; c) Purpose Specification Principle; d) Use Limitation Principle; e) Security Safeguards Principle; f) Openness Principle; Individual Participation Principle; and Accountability Principle. The previous document contains the fundamental principles setting the international standard and which should be adopted by the data protection legislation of each country. However, the document lacks a principle that establishes the protection of certain specific types of data, such as personal data that is considered sensitive, such as data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, genetic data, biometric data processed solely to identify a human being, etc. The European Union legislation collects this sensitive personal data and groups it into a specific set called "Special data categories.[172]" The reason for a separate category of this personal data is essential. It is not only necessary that companies have a lawful basis for processing listed under article 6 of the General Data Protection Regulations, but they must also have a legal basis to do it under article 9 GDPR. The reason for not including a principle of protection of sensitive personal data is straightforward. There was a conflict of views between the United States and the European Union; the difference is that the United States considers that the value of the data is given by the specific context of the data, while the European Union considers personal data as sensitive by itself[173].

The privacy guidelines issued by the OECD differ from Convention 108 in that the Convention was opened for signature during 1981 and was the first binding document regarding data protection around the world. The purpose of this convention is that its participants are required to adopt the necessary measures to apply its principles and to translate them into their legislation with the aim of ensuring respect for the fundamental rights of all individuals regarding the processing of personal data. Although Convention 108 responded to the challenges of its time, the Council of Europe decided to bring the Convention into the 21st century and update its protection with the aim of facing the challenges imposed by a digital society and the use of new technologies. Among the innovations that it brings with it are the principles of proportionality and minimization of data; legality of the processing; obligation to declare data breaches; new rights for people in

[172] European Parliament and of the Council of Europe. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Article 9.

[173] Roos, A. (2006). Core principles of data protection law. *The Comparative and International Law Journal of Southern Africa, 39(1). pp 121-122.*

an algorithmic decision-making context; accountability of data controllers; etc[174].

There are researchers who point out that data privacy laws have been proclaimed in more than 124 countries where the vast majority have followed the European standard of protection[175]. In addition, it points out that Convention 108 is an open convention that has a European origin, but that any country can apply to access[176]. There is a trend that hopes that Convention 108 has the potential to become the first treaty at an international level that promotes data protection, and that also the unique and most effective strategy that the United Nations can adopt to strengthen national legislation and the regulatory frameworks regarding the collection, processing and use of personal data is to adopt Convention 108[177]. There is a current problem in the international sphere where there is no international regulatory framework regarding the protection of personal data, and therefore there is no model to follow. This causes countries to look for a unique and unique way of dealing with this problem, so there will be discrepancies in the way that data protection is addressed.

Currently, there are 3 models to follow regarding the protection of data privacy. However, the author of this thesis will address 2 of them concerning western countries. The author of this thesis considers that the European approach to data protection has more robust protection towards the fundamental rights and liberties of people in contrast to the American approach that seems to lack this protection. The US model in terms of data protection seems to have a less protective role compared to the European model since it lacks a comprehensive national data protection law, and in addition, the different laws established regarding data protection are found distributed in the different states that make up its territory, and therefore it is difficult to follow. In contrast, the European model headed by the General Data Protection Regulation seems to be the model to be followed by various legislatures in the absence of a North American model[178].

---

[174] Council of Europe. Modernisation of the Data Protection "Convention 108". Council of Europe. Available at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.

[175] Greenleaf, G. (2018). The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy. *UNSW Law Research Paper No. 18-24*.

[176] Ibid.

[177] Ibid.

[178] Reinsch, W. (2018). Must Third Countries Choose Between EU or U.S. Digital Trade Protection Preferences?. Center for Strategic & International Studies. Available at https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/must-third-countries-choose-between-eu-or-us

The European model is based on the General Data Protection Regulation that has an expansive effect, that is, that the effects of the GDPR will not be contained in the European Union, but cover the entire world, therefore, the businesses that process data from of the European Union had to change or adapt their practices[179]. The expansive effect is typical of GDPR, but it is also possible to explain it through the "Brussels Effect" developed by Professor Bradford. It is pointed out that the European Union exerts its influence on the rest of the world through its standards and legal institutions[180]. Professor Bradford points out that the European Union, without the need to use international institutions or seek cooperation from other countries, has a growing ability to enact regulations that are embedded in legal systems or regulatory frameworks of developed markets, causing a kind of Europeanization of the other countries[181]. In the case of the European model of data protection, GDPR expands its application to countries outside the orbit of the European Union, and therefore companies that are affected by GDPR will have to change their policies and / or practices regarding the data protection. The change in practices not only occurs in foreign companies but also influences policies to promote much more robust and effective data protection.

On the one hand, the "Brussels effect" plus the expansive effect of the GDPR causes the behaviour of foreign companies to be affected, but it has also been seen that foreign legal systems have adopted European guidelines regarding privacy. Professor Greenleaf points out through his studies that the implementation of European principles regarding data privacy in countries outside the European Union continues to be substantial[182]. The result of the investigation shows that significant countries in terms of the highest GDP outside the European Union have implemented on average 5.95 out of 10 European principles regarding data privacy[183]. There are several reasons why it is possible to explain why countries outside the European Union decide to implement foreign principles or basically transplant laws from one country to another. On the one hand, the monetary aspect is evident since it is not

[179] GÜN+PARTNERS. (2016). The New EU General Data Protection Regulation with an Extra-Territorial Effect. GÜN+PARTNERS. Available at https://gun.av.tr/tr/goruslerimiz/makaleler/the-new-eu-general-data-protection-regulation-with-an-extra-territorial-effect

[180] Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review, Vol. 107, No. 1, 2012.*

[181] Ibid.

[182] Greenleaf, G. (2017). 'European' Data Privacy Standards Implemented in Laws Outside Europe. *(2017) 149 Privacy Laws & Business International Report 21-23.*

[183] Ibid

necessary to spend money looking for an adequate way to create a law, saving money when taking a foreign law and applying it saves time, money, and also the trial and error methodology. It is clear that the aspect of transplanting legislation from one country to another produces positive effects and minimizes adverse effects since it is possible to learn from the mistakes of other countries and overcome problems effectively because those problems have already been faced previously.

The American model lacks a comprehensive system for regulating data protection. When analyzing the North American system, it is possible to realize that it is regulated explicitly across sectors, such as HIPAA, which is the regulation that stipulates how personally identifiable information maintained by healthcare and policyholders must protect it from theft and fraud; FERPA is a federal law that aims to protect the privacy of student education records; COPPA is a federal law that imposes specific requirements on the operators of websites or online services that aim to protect the personal information of children under the age of 13, etc. The North American system has a limited scope, and it is not possible to observe a legal structure, nor a data protection law that is applied in the entire territory. On the other hand, the European model does have a complete data protection system that can influence countries outside the European Union, that it is possible to regulate global markets through data protection, and that it also provides many more guarantees regarding fundamental rights towards its users.

It is irrelevant to the author of this thesis whether the European Union has a direct intention to seek replication of its model in countries outside the European Union. However, it is not possible to deny the benefits of adopting similar policies regarding data protection for the European Union. One of the apparent benefits is that cooperation between businesses is facilitated since they are governed by the same law. In addition, the fact that countries outside the European Union follow the EU data protection model brings benefits in terms of the protection of fundamental guarantees, such as art 8 EU Charter.

3.2 European Union model contrasted with the United States model.

The current European model is based on the General Data Protection Regulation (“GDPR”) that came to replace the European Data Protection Directive 95/46/EC. The directive establishes a minimum of data privacy and security standards in which each member state

of the European Union should implement it in its legislation[184]. However, the board was unable to meet the challenges of modern society such as using the bank online, social networks began to be used on a massive scale, and privacy around large companies began to be affected[185].

As previously seen, the protection of privacy and the protection of personal data are enshrined at the constitutional and human rights level. Article 8 of the EU Charter establishes the right to the protection of personal data in which there must be processing with a legitimate basis, the right to access that data, to be rectified, etc. Furthermore, Article 8 ECHR establishes the right to privacy and family life.

While the European Union bases its personal data protection on fundamental rights, the protection of data in the United States is primarily based on the protection of consumers against unfair practices[186]. The United States Constitution does not have an express reference to the right to privacy or data protection, but through its Fourth Amendment, the citizens of the United States are protected against the unreasonable searches and seizures made by the United States government. As previously developed, the United States Supreme Court justices have developed through jurisprudence a right to privacy for citizens of the United States. The above presents a problem, and one would tend to think that the Supreme Court Justices are filling the gaps that the law has left without protection, however, it is evident that the United States Constitution plus the work of the Judges of the Court Suprema and its jurisprudence cannot grant adequate protection to people's privacy taking into account the technological advances that exist. The recent cases of the Supreme Court[187] demonstrate that there is an evident outdating on the part of the precepts created during the 20th century when it comes to being applied to cases concerning 21st-century technology.

[184] European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

[185] Yulia Vangorodska, ESQ. Google Sued For Illegally Scanning Emails. Yulia Vangorodska, ESQ. New York Commercial Litigation. Available at https://www.nylitigationfirm.com/google-sued-for-illegally-scanning-emails/.

[186] ICLG. USA: Data Protection 2019. The International Comparative Legal Guides. Available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[187] McCubbin, S. (2018). Summary: The Supreme Court Rules in Carpenter v. United States. Lawfare. Available at https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.

Professor Schwartz points out that although the United States played a crucial role in the international sector in terms of development and debates around privacy, the rest of the world has followed the model of the European Union establishing laws to protect the personal data European style[188]. However, despite the leading role that the United States had when discussing privacy in the international sphere, it has been observed that to date there is no general law on data protection, but rather various laws that regulate sectors specific data.

Although there is no general federal law on data protection, there are federal data protection laws that usually are concerned with the protection of specific sectors:

The Family Educational Rights and Privacy Act ("FERPA")[189] provides protection to students for the purpose of granting inspection and review rights with the goal of keeping the student's records as accurate as possible, and the disclosure of those records or personal information without the consent of the student or parent is also prohibited; The Health Information Portability and Accountability Act ("HIPAA")[190] provides protection to the information maintained by health related institutions, provision of health care services or payment that are linked to a person; The Telephone Consumer Protection Act ("TCPA")[191] It is intended to regulate phone calls and text messages made for marketing purposes or using automatic dial systems, or pre-recorded messages; The Fair and Accurate Credit Transactions Act ("FACTA")[192] It has the objective of restricting the use of the information of a subject referring to the credit capacity, general reputation, credit worthiness, credit standing; The Gramm Leach Bliley Act ("GLBA")[193] has the objective of regulating the obligations regarding the disclosure of personal information (Non-Public Personal Information) in the hands of banks, insurers and other financial companies. There is a range of laws that seek the protection of specific sectors, such as personal information, video rental records, family, telephone, etc[194].

---

188 Schwartz, P. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. 126 Harvard Law Review 1966.

189 20 U.S. Code § 1232g. "Family educational and privacy rights"

190 29 U.S. Code § 1181. "Increased portability through limitation on preexisting condition exclusions"

191 47 U.S. Code § 227. "Restrictions on use of telephone equipment"

192 15 U.S. Code § 1681. "Congressional findings and statement of purpose"

193 15 U.S. Code § 6802. "Obligations with respect to disclosures of personal information"

194 Levin, A., Nicholson, M. (2006). Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground. *University of Ottawa Law & Technology Journal, Vol. 2, No. 2, pp. 357-395, 2005.*

Although there is a specific sector regulation at the federal level, states can enact laws that impose more significant restrictions and obligations on businesses that seek the collection, processing, use of special categories of information such as medical records, biometric data, among other data categories[195]. In addition, all states have enacted data breach notification laws that apply to residents of those states. What is unique about these regulations is that even if a business does not have a physical presence in those states, they must comply with that law when they are faced with unauthorized access by residents of specific states[196].

The United States' approach to personal data protection is difficult to understand. At first glance, it is possible to argue that the regulatory system of data protection is focused on sector laws, focused on consumers and voluntary regulation, in these cases it is not possible to speak of adequate protection for personal data of individuals. When we analyze the European case, GDPR is the general norm that regulates data protection; therefore, its regulation is quite uniform throughout the member states. Now, it is possible to verify that there are different positions in the fundamental protection granted by both systems. However, one problem that is evident in the system imposed in the United States is that there is no clear definition of the terminology used in its approach through sectoral laws. For example, in the case of personal data, the United States refers to personal information, since its definition is not uniform throughout the states and their regulations; Certain data may be considered personal information for some purposes, but not for others[197]. In the case of the European Union, personal data is defined as any information related to the identification of a natural person[198]. The terminology of processing, controller, processor is not applicable in the system of the United States[199].

The federal and / or state laws of the United States do not have uniform concepts that

[195] See more, 740 ILCS 14/ "Biometric Information Privacy Act"; Tex. Bus. & Com. Code §503.001 "Capture or Use of Biometric Identifier"; Wash. Rev. Code Ann. §19.375.020 "Enrollment, disclosure, and retention of biometric identifiers".

[196] NCSL. (2020). Security Breach Notification Laws. NCSL National Conference of State Legislatures. Available at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[197] ICLG, supra note 186.

[198] 12) European Parliament and of the Council of Europe. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[199] ICLG, supra note 186.

facilitate the understanding of its rules. Moreover, the federal and state laws of the United States do not agree in a proper term that identifies an essential category such as what is understands personal information[200]. Professor Schwartz and Solove correctly point out that the approach of the United States model to the European Union model contains similarities and differences, for example, the principles of data minimization, transparency and data quality exist in both legal systems, while the automated decision-making principles, the need for a legal basis for data collection and processing, restriction on data transfers, additional protection for sensitive data cannot be found in the United States model, but in the European Union[201].

It is clear that the European Union and the United States have different philosophies regarding privacy and the protection of personal data[202]. Despite the fact that the laws of the European Union and the States are beginning to use the same language regarding data protection, it is still possible to find significant differences[203]. The underlying problem that exists today in the United States is that the protection of personal data does not seek its protection as in the European Union since while the European Union sees the protection of the privacy of personal data as a fundamental right, The United States does not see it this way. It seems that the United States system has chosen to have a protection system for personal data focused on sectors and not opting for a comprehensive data protection system as the model of the European Union since it seeks to avoid a conflict of interests, a clash between rights.

The point of view of the author of this thesis is that the prevailing system in the United States offers rather vague protection to natural persons, and also does not change the conduct of business when operating in the processing of personal data. However, there seems to be hope in the latest laws enacted in the United States, such as the California Consumer Privacy Act ("CCPA")[204] that seems to approach the European Model.

---

[200] Schwartz, P., Solove, D. (2014). Reconciling Personal Information in the United States and European Union. *California Law Review, 102(4), 877-916.* Retrieved April 19, 2020, from www.jstor.org/stable/23784355

[201] Id. at 900-904.

[202] Zanfir, G. (2012). EU and US Data Protection Reforms: A Comparative View. *EIRP Proceedings, Vol 7 (2012).*

[203] Id.

[204] Cal. Civ. Code §1798.100, "California Consumer Privacy Act".

3.3 A common point between both models.

The question to answer now is whether the European model has influenced the model of the United States, or if there are signs that the American model is adopting principles of the European model. It has already been explained previously that the model of the United States is characterized by enacting laws for specific sectors, and that in addition its personal data protection system is divided into different federal and / or state laws. Although there are no efforts by the federal power to enact robust data protection laws, it has been the different states that have sought the enactment of laws that seek the protection of personal data, resembling the style of the European model.

The state of California recently enacted a law in 2018 that creates new rights for consumers regarding elimination, and the sharing of personal data that different businesses collect from their consumers. The law in question is the California Consumer Privacy Act ("CCPA")[205] with the objective of providing more robust protection in terms of protecting the data of California consumers. However, CCPA is not the first effort by this State to grant a victory in the search for greater protections to the privacy of the people since in 1972 the right to privacy was included in the Constitution of the State of California[206].

California is one of the 10 states to enshrine the right to privacy at the level of its constitution[207]. That can be set a precedent and a state commitment to the importance of people's privacy. The first draft of CCPA was born as an initiative to grant three fundamental rights to California consumers:

a) The right to know what kind of data businesses had collected about them; where they had got this information from; and also, how this data was to be used, sold, or disclosed;
b) A right for consumers to "opt-out" of the sale or disclosure of that data for commercial purposes;

[205] *Id.* at §1798.100-199
[206] Clark Kelso, J. (1992). California's Constitutional Right to Privacy. *19 Pepp. L. Rev. Iss. 2*. Available at: https://digitalcommons.pepperdine.edu/plr/vol19/iss2/1
[207] NCSL. (2018). Privacy Protections in State Constitutions. NCSL National Conference of State Legislatures. Available at http://www.ncsl.org/research/telecommunications-andinformation-technology/privacy-protections-in-state-constitutions.aspx.

c) and also, the right to be able to sue the businesses that were against these rights[208].

A.B. 375 retains the fundamental rights enshrined in the first draft, but rights were also added to people seeking to know what kind of personnel data it is collecting about them; know if that personal data will be sold or disclosed; know to whom that personal data will be sold or disclosed; to refuse or refuse on the sale of this personal data, and in the case of refusing it, the right to the same service is protected in equal conditions and price with respect to the people who did not refuse[209].

The California Consumer Privacy Act can be understood as the fruit of the influence of the European model on the model of the United States. However, despite the consecration of specific rights in CCPA similar to those contained in the General Data Protection Regulation, it is possible to find specific differences.

The first thing to note is the scope of both standards, on the one hand, we are talking about CCPA that defines a consumer as "a natural person who is a California resident"[210] while GDPR does not have as a requirement the residence of a particular state. CCPA generally applies to businesses that collect personal data from consumers who do business in the State of California, and who meet any of the requirements of having annual gross revenue of 25,000,000, buy, sell, receive or share for purposes commercials the information of more than 50,000 consumers California residents[211]. The point in common here with GDPR is its extraterritoriality. However, scopes of the type of health information are not contained in CCPA, while in GDPR, they are covered.

CCPA is an unanticipated result of United States law, which restores rights to consumers, and not only seeks transparency in the data processing. It is possible to point out that CCPA has much more in common than GDPR than the other privacy laws of the United States[212].

[208] Ross, M., Mactaggart, A. (2017). "The Consumer Right to Privacy Act of 2018" – Version 2 No. 17-0039. *CAL. OFFICE OF THE ATT'Y GEN.* Available at https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf

[209] Cal. Civ. Code §1798.100, "California Consumer Privacy Act".

[210] *Ibid.*

[211] *Id.*at §1798.140

[212] Kalyvas, J., Millendorf, S., Overly, M., Ridley, E., Surpin, B., Howell, C., Rathburn, J., Tantleff, A. (2018). California Moves Towards GDPR-Like Privacy Protections in the California Consumer Privacy Act of 2018.

However, despite CCPA seeking to empower consumers with regard to their information and California being the fifth largest economy in the world[213], CCPA does not prevent businesses from stopping to collect information from California consumers, nor does it give them the opportunity to stop the collection of personal data information.

Although there are differences between GDPR and CCPA, it is necessary to focus on the similarities of CCPA with the European model. The definitions of personal information and personal data are quite similar in both regulations, an example of this is that CPPA defines personal information as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"[214] while GDPR defines personal data in Art. 4 (1), "Personal data are any information which is related to an identified or identifiable natural person"[215]. Both regulations are also similar in terms of the rights they grant their individuals, pseudonymization and special protection for children. The right to information is found in both legal bodies in which it is sought that the end-user of the right is informed about the type of data that is being collected, with what scope and for what purpose. Both mechanisms oblige the entities to put mechanisms in place regarding the activation of these rights by the indicated persons, portability of the data and rectification of it.

As the author of this thesis has previously pointed out, it is not possible to say that the GDPR and the CCPA have the same powers, but rather it is possible to observe an approach by the CCPA towards the European model that cannot be observed in other laws of the United States.

When navigating the data protection system of the United States, it is possible to observe a large number of laws focused on data protection but in a focused way across sectors. However, it is possible to observe a tendency to create new legislation that covers the United

FOLEY & LARDNER LLP. Available at https://www.foley.com/california-moves-towards-gdpr-like-privacy-protections-in-thecalifornia-consumer-privacy-act-of-2018-07-02-2018/

[213] Ximénez de Sandoval, P. (2018). California ya es la quinta mayor economía del mundo. El País. Available at https://elpais.com/elpais/2018/05/09/opinion/1525882179_659426.html.

[214] 19) Cal. Civ. Code §1798.140, "California Consumer Privacy Act".

[215] 12) European Parliament and of the Council of Europe. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Article 4(1).

States in general[216]. However, this would raise many questions as to how a federal level law would exceed the laws of the states. A law on the protection of personal data of a national nature would totally change the approach that the United States has had towards data protection, it would bring much more clarity to its system characterized by regulation across sectors. It is not talking about granting greater protections to the citizens of the United States but would change the model of the United States through the regulation of sectors towards a generalized model like the European model.

[216] Wagner, A., Arensberg, T. (2020). Proposed Legislation for Security in the Digital Age. JDSUPRA. Available at https://www.jdsupra.com/legalnews/proposed-legislation-for-security-in-55807/

CONCLUSION

This thesis has sought to draw a parallel between the right to data protection in the model of the United States and the model of the European Union. Both models have different characteristics marked explicitly by the way in which the right to privacy is understood.

On the one hand, in the United States model, the right to privacy is not explicitly enshrined in its Constitution, in which U.S. Justice Louis Brandeis referred to the right to privacy as the right to be left alone, and throughout the course of the 20th century, the Supreme Court of the United States provided people with some protection of privacy through various amendments. On the other hand, the European Union model makes an express recognition of the right to privacy in both Article 8 ECHR and Article 7 EU Charter.

The right to privacy contains a belief that seeks to restrain the involvement of the government and private actors towards the private affairs of individuals. In the past, the right to privacy could be dealt with from a much more closed spectrum, since technology at that time did not pose a significant threat. However, today we live in a modern society in which the individuals of a society are continually handing over personal data to companies in order to receive a service. The above presents a series of risks since devices such as a simple cell phone collect data from its users at levels never thought before. The majority of government institutions or private institutions are the actors that threaten the right to privacy in a modern era such as the one in which we live. Concerns have escalated to a higher level when we see that companies like Cambridge Analytica have used the data collected by Facebook to influence the political decisions of large numbers of people.

When living in a modern society with new technologies, there must be a balance between privacy and how we disclose information to third parties, after all, the right to privacy is a personal right, and also a human right. The collection of personal data is placed as a threat to this privacy; therefore, data protection regulations are of utmost importance. Data protection can be a broad term, but it regularly includes the collection, use, and dissemination of individuals' personal information. The primary purpose of the protection of personal data is not only its protection but also the protection of the fundamental rights and freedoms that correspond to the person who corresponds to that data. As we have pointed

out before, there is an express recognition of privacy and the right to data protection in international treaties.

Data is becoming a precious commodity in which it is in constant movement with the aim of providing services. The data processing that occurs today increases the difficulty for people to maintain control over their personal data that they are sharing with different companies. Data protection refers to the system of practices, assurances, rules, procedures, etc. that seek to protect them. Each legislation can adopt different regulations that contain the necessary mechanisms for data protection. However, today there are two models of personal data protection that have established themselves as the main actors in the international sphere. The United States model is characterized by regulation of specific data sectors that are difficult to follow and only provides minimal protection in terms of data protection. While the European Union model focuses on the regulation of data protection in a general and easily understood way. Now, the model of the European Union has positioned itself as a benchmark for various laws. Third world countries have sought to guide their model to data protection taking the European Union model as a reference because it is much cheaper to implement a model that has already been proven effective. In addition, the European Union has managed to impose its influence to export the protection of fundamental rights and freedoms to other sectors outside the European Union. This can be explained on the basis that to date, the European Union model in terms of data protection, has been the most effective when compared to the United States model.

The United States has had a crucial role in the international sector in developing the debates regarding privacy; however, the rest of the world has followed the model of the European Union because the approach of the United States is hard to understand. First, there is no general regulation on the protection of data, but we find a multiplicity of laws concentrated in different sectors, concentrated on consumers and a voluntary regulation that does not present the necessary guarantees to protect personal data from users.

It is true that a different approach to data protection is possible, but the regulation proposed by the United States has not solved fundamental problems such as a uniform definition of personal data or the existence of cases that data can be considered as personal or not. However, although there are fundamental differences in data protection in the model of the United States and the European Union, there are also certain similarities in which the

principles of data minimization, transparency and data quality are found in both models.

The United States model offers quite a precarious protection to natural persons and fails to significantly influence business conduct, while the European Union system seeks the protection of data as a human right since managed to shape business conduct. Although there is a multiplicity of models, the two models that have managed to position themselves as referents have been two, the model of the United States and the model of the European Union. The last question that has been answered is about why the model of the European Union has become a benchmark for countries outside the European Union to influence the model of the United States.

As previously demonstrated, there have been no efforts by the federal power to enact laws that seek to strengthen data protection, but rather the states themselves have sought to enact laws that seek to strengthen data protection. data protection similar to the model of the European Union. One of these states is the state of California.

The State of California enacted during the year 2018 the California Consumer Privacy Act with the objective of promoting robust protection regarding the protection of the data of California consumers. California is considered the fifth economy in the world, and CCPA is not its first victory in terms of privacy since it is one of the 10 states that has recognized the right to privacy at a constitutional level.

It is possible to observe an approach to the model of the European Union through the legislative work of the States. Recent developments in data protection at the state level give clear indications of an approach of the United States model towards the European model. However, although it is possible to argue that CCPA has much more in common with GDPR than other privacy laws in the United States, CCPA does not stop businesses from continuing to collect information from California consumers and / or does not give them an opportunity to stop data collection.

It is not possible to maintain that GDPR and CCPA are sister laws that grant the same powers and value the system to data protection in the same way, but it is possible to observe an approach of the state of California to the model of the European Union that makes one think that this type of enactment of laws will be replicated throughout the United States.

It is still necessary to observe the development and influence that CCPA will have on the other States in the United States. California has been a leader in privacy protection in the past, but it remains to be seen how the relationship between businesses and their clients will develop in the future. If the steps taken by California are analysed, similar paths will be taken in other States. However, federal legislation needs to provide a set of rules that meets the expectations of United States citizens and the principles of Human Rights.

We are in a unique situation in which there is an opportunity to seek the protection of our privacy, and of our digital identity with which we interact day by day. It is necessary that the States take the central role when searching for the protection of personal data, and that businesses are able to recognize and follow these rules.

ABBREVIATIONS

ACHR	The American Convention on Human Rights.
CCPA	California Consumer Privacy Act.
CJEU	Court of Justice of the European Union.
CRC	Convention on the Rights of the Child.
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms.
ECtHR	European Court of Human Rights.
EU Charter	Charter of Fundamental Rights of the European Union.
GDPR	General Data Protection Regulation.
IACtHR	The Inter-American Court of Human Rights.
ICCPR	The International Convention on Civil and Political Rights.
ICRMW	International Convention on the protection of All Migrant Workers and Member of their Families.
OAS	Organization of American States.
OECD	Organization for Economic Cooperation and Development.
UDHR	Universal Declaration on Human Rights.
UN	United Nations.

REFERENCES

BOOKS AND ARTICLES

1. Warren, S. D;, Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, Vol. IV. Available at http://links.jstor.org/sici?sici=0017811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C.
2. Granger, M.-P., and Irion, K. (2018). 'The right to protection of personal data: the new posterchild of European Union citizenship?' in: de Vries, S., de Waele, H., and Granger, M.-P., eds., Civil Rights and EU Citizenship (Cheltenham: Edward Elgar Pub.).
3. Onn, Y. (2005). Privacy in the Digital Environment. Haifa Center of Law & Technology. Retrieved from http://law.haifa.ac.il/images/Publications/Privacy_eng.pdf.
4. de Montjoye, Y., Hidalgo, C., Verleysen, M. (2013). Unique in the Crowd: The privacy bounds of human mobility. Sci Rep 3, 1376. https://doi.org/10.1038/srep01376.
5. Seneviratne, S., Seneviratne, A., Mohapatra, P. and Mahanti, A. (2014). Predicting user traits from a snapshot of apps installed on a smartphone. ACM SIGMOBILE Mobile Computing and Communications Review, 18(2), pp.1-8. http://dl.acm.org/citation.cfm?id=2636244.
6. Min, J. K., Wiese, J., Hong, J.I. and Zimmerman, J. (2013). Mining smartphone data to classify life-facets of social relationships. ACM SIGMOBILE Mobile Computing and Communications Review, pp. 285-294. Available at http://dl.acm.org/citation.cfm?id=2441810.
7. Shawn, M. B. (2017). Data Protection in the United States: U.S. National Report. Indiana University Robert H. McKinney School of Law Research Paper No. 2017-11.
8. Hamm, R. F. (2010). Olmstead v. United States: The Constitutional Challenges of Prohibition Enforcement. University at Albany, SUNY, Edited by the Federal Judicial Center for inclusion in the project Federal Trials and Great Debates in United States History.

9. Issacharoff, L.; Wirsha, K. (2016). Restoring reason to the third-party doctrine. Minnesota Law Review, 100(3).
10. Gentithes, M. (2020). App permissions and the third-party doctrine. Washburn Law Journal, 59(1).
11. Kerr, O. S. (2009). The case for the third-party doctrine. Michigan Law Review, 107(4).
12. van der Sloot, B., (2015). Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data". Utrecht Journal of International and European Law, 31(80), pp.25–50. Available at http://doi.org/10.5334/ujiel.cp.
13. Bygrave L. (2010). Privacy and Data Protection in an International Perspective. Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010. Available at https://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf.
14. Thompson, A. (2008). The United States and the ICCPR. SAIS Review of International Affairs 28(2). pp 105-106. Available at https://muse.jhu.edu/article/254270/pdf.
15. Swire, P., Kennedy-Mayo, D. (2016). How Both the EU and the U.S. Are 'Stricter' Than Each Other for the Privacy of Government Requests for Information. 66 Emory Law Journal 617 (2016).
16. McGeveran, W. (2016). Friending the Privacy Regulators. 58 ARIz. L. REV. 959.
17. Lynskey, O. (2014). Deconstructing data protection: The added-value of right to data protection in the EU legal order. International and Comparative Law Quarterly, 63(3).
18. González, G., Gellert, R. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. International Review of Law, Computers & Technology, 26:1.
19. Ganotra, S. (2018). Gdpr compliant or not. Court Uncourt | STA Law Firm: Volume V Issue VI.
20. Roos, A. (2006). Core principles of data protection law. The Comparative and International Law Journal of Southern Africa, 39(1).
21. Greenleaf, G. (2018). The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy. UNSW Law Research Paper No. 18-24.

22. Bradford, A. (2012). The Brussels Effect. Northwestern University Law Review, Vol. 107, No. 1, 2012. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770634.
23. Greenleaf, G. (2017). 'European' Data Privacy Standards Implemented in Laws Outside Europe. (2017) 149 Privacy Laws & Business International Report 21-23. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3096314.
24. Schwartz, P. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. 126 Harvard Law Review 1966. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2290261.
25. Levin, A., Nicholson, M. (2006). Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground. University of Ottawa Law & Technology Journal, Vol. 2, No. 2, pp. 357-395, 2005. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=894079.
26. Schwartz, P., Solove, D. (2014). Reconciling Personal Information in the United States and European Union. California Law Review, 102(4), 877-916. Available at www.jstor.org/stable/23784355.
27. Zanfir, G. (2012). EU and US Data Protection Reforms: A Comparative View. EIRP Proceedings, Vol 7 (2012).
28. Clark Kelso, J. (1992). California's Constitutional Right to Privacy. 19 Pepp. L. Rev. Iss. 2. Available at: https://digitalcommons.pepperdine.edu/plr/vol19/iss2/1.
29. American Jurisprudence 2d (Am Jur 2d) (1962).
30. Weil, G. L, & Goodrich, L. M. (1963). The European convention on human rights: background, development and prospects. Leyden: Sythoff.
31. Tessaro T., Trojani F. (2006), Privacy e accesso ai documenti nell'Ente locale. Maggioli Editore
32. Bygrave, L. (2002). Data Protection Law: Approaching its Rationale, Logic and Limits (Information Law Series Set). Kluwer Law International.
33. DLA Piper's Data Protection, Privacy & Security group. (2014). Data Protection Laws of the World Handbook. Available at https://www.dlapiperdataprotection.com/
34. Canton, S. (2002). The Role of the OAS Special Rapporteur for Freedom of Expression in Promoting Democracy in the Americas. 56 U. MIAMI L. REV. 307, 309.

35. Wippman, D., Dunoff, J. L., & Ratner, S. R. (2006). International Law: Norms, Actors, Process: A Problem-oriented Approach. (2nd Edition ed.) Aspen Publishers.
36. Raul, A., Manoranjan. T., Mohan, V. (2015). THE PRIVACY, DATA PROTECTION, AND CYBERSECURITY LAW REVIEW. Law Business Research Ltd, London. pp 268-269.
37. Rouvroy A., Poullet Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht.

CASE LAW

38. Stanley v. Georgia, 394 U.S. 557 (1969).
39. Roe v. Wade, 410 U.S. 113 (1973).
40. United States v. Miller, 307 U.S. 174 (1939).
41. Olmstead v. United States, 277 U.S. 438 (1928).
42. National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958).
43. Talley v. California, 362 U.S. 60 (1960).
44. Watkins v. United States, 354 U.S. 178 (1957).
45. Agnello v. United States, 269 U.S. 20 (1925).
46. Gouled v. United States, 255 U.S. 298 (1921).
47. Amos v. United States, 255 U.S. 313 (1921).
48. Silverthorne Lumber Co., Inc. v. United States, 251 U.S. 385 (1920).
49. Weeks v. United States, 232 U.S. 383 (1914).
50. Boyd v. United States, 116 U.S. 616 (1886).
51. Ex parte Jackson, 96 U.S. 727 (1878).
52. Poe v. Ullman, 367 U.S. 497 (1961).
53. Griswold v. Connecticut, 381 U.S. 479 (1965).
54. Katz v. United States, 389 U.S. 347 (1967).
55. Goldman v. United States, 316 U.S. 129 (1942).
56. United States v. Miller, 425 U.S. 435 (1976).
57. Smith v. Maryland, 442 U.S. 735 (1979).

58. United States v. Jones, 565 U.S. 400 (2012).
59. Riley v. California - 134 S. Ct. 2473 (2014).
60. Bond v. U.S., 529 U.S. 334 (2000).
61. Stoner v. California, 376 U.S. 483 (1964).
62. Carpenter v. United States, No. 16-402, 585 U.S. ____ (2018).
63. ECtHR 13710/88, Niemietz v. Germany.
64. ECtHR 44647/98, Peck v. The United Kingdom.
65. ECtHR 33810/07, Association "21 December 1989" and Others v. Romania.
66. ECtHR 27798/95, Amann v. Switzerland.
67. ECtHR 9248/81, Leander v Sweden.
68. ECtHR 7215/75 X v. United Kingdom.
69. ECtHR 74336/01, Beteiligungen GmbH v. Austria.
70. CJEU Case 136/79, National Panasonic (UK) Limited v. Commission of the European Communities.
71. ECtHR 28341/95, Rotaru v Romania.
72. IACtHR Judgment of July 6, 2009, Escher et al.v. Brazil.
73. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland.
74. ECtHR 57375/08, P. and S. v. Poland.
75. ECtHR 588/13, Libert v. France.
76. ECtHR 61496/08, Bărbulescu v. Romania.
77. ECtHR 5786/08, Söderman v. Sweden.
78. ECtHR 40660/08 and 60641/08, Von Hannover v. Germany.
79. CJEU, Joined Cases C–92/09 and C–93/09 Volker und Markus Schecke.
80. CJEU ECR I-11063, Eifter.

LEGAL ACTS

81. Lei Nº 13.709, (14th of August 2018). República Federativa de Brasil.
82. U.S. Const. amend I.
83. Connecticut Public Acts 1879, c. 78.
84. Articles 53-32, 54-196 of The General Statutes of Connecticut (1958 rev.).
85. 18 U.S. Code § 1084.Transmission of wagering information; penalties.
86. Senate Executive Report. (1992) No. 102-23.

87. Public Law 104–191, “Health Insurance Portability and Accountability Act of 1996”.
88. 20 U.S. Code § 1232g, “Family educational and privacy rights”.
89. 5 U.S.C. § 552a, “Records maintained on individuals”.
90. Public Law 107-347, “The Federal Information Security Management Act of 2002”.
91. 15 U.S.C. § 1681, “Congressional findings and statement of purpose”.
92. 15 U.S. Code § 41. “Federal Trade Commission established; membership; vacancies; seal”.
93. 29 U.S. Code § 1181. “Increased portability through limitation on preexisting condition exclusions”.
94. 47 U.S. Code § 227. “Restrictions on use of telephone equipment”.
95. 15 U.S. Code § 6802. “Obligations with respect to disclosures of personal information”.
96. 740 Illinois Compiled Statues 14 “740 ILCS 14/” “Biometric Information Privacy Act”.
97. Texas Business & Commercial Code §503.001 “Capture or Use of Biometric Identifier”.
98. Washington Revised Code Ann. §19.375.020 “Enrolment, disclosure, and retention of biometric identifiers”.
99. California Civil Code §1798.100, “California Consumer Privacy Act”.

TREATIES

100. United Nations. (1948). Universal Declaration of Human Rights.
101. Council of Europe., & Council of Europe. (2000). The Charter of Fundamental Rights of the European Union.
102. United Nations, General Assembly. (1966). International Covenant on Civil and Political Rights.
103. United Nations, General Assembly. (1990) International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families.
104. United Nations, General Assembly. (1989). Convention on the Rights of the Child.
105. Council of Europe., & Council of Europe. (1952). The European convention on human rights. Strasbourg: Directorate of Information.

106. Organization of American States (OAS). (1969). American Convention on Human Rights, "Pact of San Jose".

107. United Nations Human Rights Committee (HRC). (1988) CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation

108. 35th International Conference of Data Protection and Privacy Commissioners Privacy: A compass in turbulent world. Warsaw, 23-26 September 2013.

109. European Union. (2007). the Treaty on the Functioning of the European Union

110. European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

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

112. Council of the European Union. (2015). 9565/15, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Available at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

113. Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe Treaty Series 108. Strasbourg: Council of Europe.

114. Organization for Economic Cooperation and Development. (2013). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.

OTHER SOURCES

115. BBC Mundo. 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. BBC. https://www.bbc.com/mundo/noticias-43472797.

116. Computer Hope. Social network. Computer Hope Free computer help since 1998. https://www.computerhope.com/jargon/s/socinetw.htm.

117. GVZH. Data Protection vs. The Right to Privacy. GVZH Advocates. https://www.gvzh.com.mt/malta-law/data-protection/vs-the-right-to-privacy/.

118. Privacy International. PRIVACY AND HUMAN RIGHTS An International Survey of Privacy Laws and Practice. Global Internet Liberty Campaign. http://gilc.org/privacy/survey/intro.html.

119. Solove, D. J. (2010). The meaning and value of privacy appeal for a pluralistic definition of the concept of privacy. Open! Platform for Art, Culture & the Public Domain. https://onlineopen.org/the-meaning-and-value-of-privacy.

120. Smith, A. (2017). Americans and Cybersecurity Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives. Pew Research Center. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.

121. Lee, R. (2013). Cell phone ownership hits 91% of adults. Pew Research Center. https://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

122. Menand, L. (2018). Why do we care so much about privacy?. The New Yorker. https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy.

123. Katz v. United States. (n.d.). Oyez. Retrieved April 27, 2020, from https://www.oyez.org/cases/1967/35.

124. Cheng, R. (2018). Say the Secret Word: Court Allows Cellphone Search Despite Password Request before Miranda Warning. Forbes. https://www.forbes.com/sites/roncheng/2018/08/09/say-the-secret-word-court-allows-cellphone-search-despite-password-request-before-miranda-warning/#2b2d18af771d.

125. European Court of Human Rights. (2019). Guide on Article 8 of the European Convention on Human Rights, Right to respect for private and family life, home and correspondence. https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

126. Frontier Technology. (2015). The differences between EU and US data laws. Frontier Technology. https://www.frontiertechnology.co.uk/differences-between-eu-and-us-data-laws.

127. United Nations Human Rights Office of the High Commissioner. Status of Ratification. Ratification of 18 International Human Rights Treaties. Available at https://indicators.ohchr.org/.

128. European Commission. Data protection in the EU. European Commission. Available at https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

129. Organization for Economic Cooperation and Development. OECD work on privacy. OECD. Available at http://www.oecd.org/sti/ieconomy/privacy.htm.

130. Council of Europe. Modernisation of the Data Protection "Convention 108". Council of Europe. Available at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.

131. Reinsch, W. (2018). Must Third Countries Choose Between EU or U.S. Digital Trade Protection Preferences?. Center for Strategic & International Studies. Available at https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/must-third-countries-choose-between-eu-or-us.

132. GÜN+PARTNERS. (2016). The New EU General Data Protection Regulation with an Extra-Territorial Effect. GÜN+PARTNERS. Available at https://gun.av.tr/tr/goruslerimiz/makaleler/the-new-eu-general-data-protection-regulation-with-an-extra-territorial-effect.

133. Yulia Vangorodska, ESQ. Google Sued For Illegally Scanning Emails. Yulia Vangorodska, ESQ. New York Commercial Litigation. Available at https://www.nylitigationfirm.com/google-sued-for-illegally-scanning-emails/.

134. ICLG. USA: Data Protection 2019. The International Comparative Legal Guides. Available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

135. McCubbin, S. (2018). Summary: The Supreme Court Rules in Carpenter v. United States. Lawfare. Available at https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.

136. NCSL. (2020). Security Breach Notification Laws. NCSL National Conference of State Legislatures. Available at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

137. NCSL. (2018). Privacy Protections in State Constitutions. NCSL National Conference of State Legislatures. Available at http://www.ncsl.org/research/telecommunications-andinformation-technology/privacy-protections-in-state-constitutions.aspx.

138. Ross, M., Mactaggart, A. (2017). "The Consumer Right to Privacy Act of 2018" – Version 2 No. 17-0039. CAL. OFFICE OF THE ATT'Y GEN. Available at https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf.

139. Kalyvas, J., Millendorf, S., Overly, M., Ridley, E., Surpin, B., Howell, C., Rathburn, J., Tantleff, A. (2018). California Moves Towards GDPR-Like Privacy Protections in the California Consumer Privacy Act of 2018. FOLEY & LARDNER LLP. Available at https://www.foley.com/california-moves-towards-gdpr-like-privacy-protections-in-thecalifornia-consumer-privacy-act-of-2018-07-02-2018/.

140. Ximénez de Sandoval, P. (2018). California ya es la quinta mayor economía del mundo. El País. Available at https://elpais.com/elpais/2018/05/09/opinion/1525882179_659426.html.

141. Wagner, A., Arensberg, T. (2020). Proposed Legislation for Security in the Digital Age. JDSUPRA. Available at https://www.jdsupra.com/legalnews/proposed-legislation-for-security-in-55807/.

Non-exclusive licence to reproduce thesis and make thesis public

I, Mario Antonio Alfaro Bobadilla

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

The Right to Data Protection in the US: The influence of GDPR in the US Model

Supervised by dr. iur. Paloma Krõõt Tupay.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Mario Antonio Alfaro Bobadilla

29/04/2020