LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department of Political Science
Master's Degree in International Relations
Chair of Comparative Public Law

The Law and Politics of Data Protection between the European Union and the United States

Supervisor
Prof. Cristina Fasone

Co-Supervisor
Prof. Antonio La Spina

Candidate
Olivia Zangrilli

Student Registration
636672

Academic year 2019/2020

Com'è definita l'identità?
In passato si diceva: "Io sono quello che dico di essere".
Oggi, siamo quello che Google dice che siamo.
Siamo sempre meno persone, sempre più profili.

Stefano Rodotà

Table of Contents

Introduction

The matter of personal data is one that has become increasingly relevant in recent years, in particular because of the rapid development in the field of IT.

In just two decades, there have been developments that have significantly expanded the capacity to store data and information. On the other hand, in combination with advances in the field of data storage, the spread and growth of the Internet has taken place. Nowadays, in voluminous shelves, it is no longer necessary to store thousands of pieces of paper: everything is uploaded and saved on the web and easily accessible from anywhere and exchanged quickly without geographical limitations. Finally, the proliferation of the phenomenon of social networks, the sites that par excellence see a vast amount of personal data posted every day in them and that in certain cases have blurred if not lost the conventional limits of privacy, has been seen in recent years. Social networks and search engines derive much of their profits from the selling of their users' personal data. As for businesses which have to deal with submitting IT with the management of personal data stored in servers, they often do not guarantee sufficient standards of security of the data collected, proving on more than one occasion not to be up to the role of responsible for that data.

Finally, there has been another aspect in recent years that has strongly affected this issue: terrorism. Following the September 11, 2001 attacks in the United States, greater regulation at the cost of privacy and the security of personal data was the direction taken. By comparison, the European Union (EU) has favored safeguarding the privacy of personal data. There is no globally accepted law at present on the privacy of personal data. Part of the difficulty of reaching an agreement is that it is a morally controversial area in which the right of expression has been and continues to be opposed to the right to privacy or national security against privacy.

Simplistically speaking, the right to the privacy of personal data protects the data of an individual, interpreted as that collection of information relating to various aspects of a person's life (both his private sphere and his social sphere), which the person concerned wishes to make accessible to the public or, on the contrary, decides not to disseminate.

Moreover, over time, the paradigm of privacy and the conception of personal data protection itself has changed: It has shifted from an initial, solely 'material' definition of data protection (as interpreted by the US common law system), referring to the control and protection of the right to property, to a more data protection-oriented view as a decline of the rights of freedom and integrity of the person (as understood in the continental European system). In an era such as today, in which the use and exchange of information for different purposes has reached its historical peak and is destined to increase exponentially, the importance of dominating our information assets, together with a greater awareness of the use of our personal data in a 'digital society,' are essential elements in order to protect the fundamental core of personal freedoms. Therefore, the right to the protection of personal data is a valid protection of all fundamental rights in a digital society and in technologies related to electronic communications.

If we can say, of course, that the protection of personal data is functional for the protection of an individual's privacy, understood as confidentiality and the protection of what is private, the protection of personal data is, however, more specific with regard to the concepts of the protection of private and family life, of the home and of correspondence, as enshrined in Article 8 ECHR.

At this juncture, both the European Union and the United States are aware of the delicacy of this issue and seem to be interested in ensuring appropriate data protection measures in order to maintain their stable relations, both economically and in terms of their citizens' national security and protection. Therefore, the regulatory framework, which appears to be fragmentary and heterogeneous but which, at the same time, is the protagonist of numerous legislative interventions

implemented in order to obtain a more organic system of supervision, needs to be taken into account.

To date, Europe has been a champion of the protection of personal data, and the EU has adopted a regulation that ultimately standardizes data protection legislation across its Member States. The EU is currently the only international organization in a position to initiate a process that could lead to the formation of international agreements for the protection of personal data. Therefore, it is important to achieve a shared set of rules to ensure the security of the personal data of individuals by requiring a high level of protection from those who manage that personal data.

This dissertation will analyze the recent evolution of the law on the protection of personal data both in the European landscape and also in the United States, and its relationship with the most important realities surrounding it, showing the lights and shadows faced by legislators so far, and also evaluating the contrasts with other realities around the world.

A historical overview of the birth and evolution of personal data protection will be given in the first chapter.
We will come to the experience of the totalitarian states of the early '900, starting from the common core of the *Right to Privacy*, mainly understood as *the right to be let alone*, elaborated in the famous article by Warren and Brandeis in 1890, which will significantly change the perception of the two increasingly different concepts of confidentiality and protection of personal data.

The main legislative instruments adopted over the years in the field of privacy and personal data protection in the European system will be analyzed in the second chapter.
Initially, the Community legal system, formulated from an economic incorporation point of view, did not, by specific legal provisions, recognize the

issue of privacy regulation. However, Europe has also taken measures to defend the basic principles of the individual through the jurisprudence of the courts.
There have also been several complications in the evolutionary process and in the subsequent legal recognition of the right to privacy as an independent condition worthy of protection on our continent.
There is no doubt that the tragic experiences of authoritarian regimes in the first half of the nineteenth century established and reinforced in the European mentality the importance that must be assigned to the security of the private spheres of the people.
It will analyze the importance of the principles enshrined in Directive 95/46/EC, which have long been the fundamental source of personal data protection.
Finally, the Italian experience in the field of data protection will also be analyzed along with the most important reference to privacy that can be found in Article 2 of the Constitution, which covers privacy in terms of the inviolable rights of human beings.

The third chapter will be entirely centered on the analysis of the U.S. legislative system.
The concept of privacy was born in the United States at the end of the nineteenth century to guarantee the protection of ideas and feelings as an extension of the right to private property against the increasing intrusiveness of printed paper. The protection of privacy in the federal law of the United States of America, however, is very vague and there is no clear legal definition in the federal system for the same reason. This is attributable to the fact that its concept includes many different legal situations.
The US law on the protection of personal data offers, without doubt, a more fragmented regulatory system. The Fourth Amendment to the Constitution preserves privacy and personal data at a basic level.

The fourth chapter will focus on the study of the transfer of personal data to third countries and, in particular, on the conflicts with the United States that have arisen in this respect.

It aims to examine the developments that have influenced the international regulatory scenario in the light of Edward Snowden's disclosures about the US intelligence programs, Which, in turn, developed a system capable of subverting the dynamics related to the transmission and transformation of personal data, due also to Maximilian Schrems' lawsuit against the Facebook social network.
The Privacy Shield Agreement, which came into force on 12 July 2016 and expired in 2020 with Case Schrems II, will be discussed and will demonstrate the recognition of its key points and the features that distinguish it from the previous Safe Harbor Agreement.

Lastly in the fifth chapter, I will address in a comparative framework the *right to be forgotten*.
In this context, it will evaluate whether it is possible to create a general and theoretical ideal definition of the *right to be forgotten* that would go beyond jurisdiction. The review will concentrate on the two main jurisdictions, the EU and the US, explain the definition as described by the EU, and then challenge the existing narrative that the right to be forgotten is not compatible with the US. It focuses on the assessment of the effect of the case of CJEU Google Spain-Costeja on the meaning of the term, including the review of EU and US case law.

CHAPTER 1: THE KEY CONCEPTS OF PRIVACY AND DATA PROTECTION

1.1 Concept of Privacy: Definition and Evolution

If we look for the definition of "Privacy" on the Cambridge Dictionary, we can find that it is expressed in the following way: *"The state of being alone, or the right to keep one's matters and relationships secret"*[1].

The concept of Privacy is exceptionally new and modern but, at the same time, has always been something present in human nature.

The concept of Privacy has been developing since Ancient Greece when different philosophers started to talk about the "Sense of Privacy." Aristotle was the first philosopher that made the distinction between "Polis," which is the public sphere of an individual, and "Oikos," which is the private sphere associated with domestic life[2].

This element establishes the so-called personal sphere, clearly distinct from the public and political one. It is crucial to bear in mind that men's public life involvement was of fundamental importance for the ancient Greeks. Still, they recognized the individual's need for their private sphere, to be delineated as the place where they would take care of their personal needs.

There are also several passages in the Bible where the invasion of Privacy is described. It originated in its early form, where the intrusion into someone's private sphere was accompanied by guilt and rage. It is enough to think of Adam and Eve, who began to cover their bodies with leaves to protect their secrecy[3].

Nonetheless, the concept of the "right to privacy" is attributed to the future U.S. Supreme Court Justice Louis D. Brandeis and Attorney Samuel D.

---

[1] Cambridge Advanced Learner's Dictionary 1995

[2] Arist., Pol. I 3, 1253b2-8, trad. Laurenti 1989, 8

[3] Konvitz, M. R.: Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2. (1966) p. 272.

Warren. In 1890, the two jurists published "The Right of Privacy" issue of the Harvard Law Review, which represented the first legal monograph that recognized the "*right to be let alone*"[4], which focused on the protection of individuals.

This legal monograph represents a milestone in Privacy because never the Right to Privacy was recognized. Before that, the needs of protection of private life, even though they were felt at a social level, they struggled to find legal recognition, running into the hostilities of that part of the doctrine still strongly inclined to lead them back inside the logic of different rights, such as the right to reputation and honor[5]. In "The Right to Privacy," the two jurists, appealing to the Common law and its ability to adapt to all existing changes in social life, defined within the American legal system the Right to Privacy or better defined as "*the right to be let alone*"[6].

The intent was to offer protection to the more intimate and spiritual aspects of humankind. Their main objective was to protect the supreme value of personal inviolability by abandoning the material and utilitarian logic that was predominant until then[7].

The essay's significance lies not so much in the revolutionary reach of the elaborated theory as in the critique of the previous theory and the denunciation of the inadequacy of property law schemes, violation of confidence, trust or contract, and physical infringement. It preserves the nature of the right to Privacy

---

[4] Samuel D. Warren and Louis D. Brandeis, 1860, *The Right to Privacy*, Harvard Law Review, Vol.4, No.

[5] A. Westin, *Privacy and freedom*, Atheneum, New York, 1970, p. 337, stated that a right to the Privacy, although proportionate to the mechanisms of surveillance and intrusion are known at the time, found recognition in American law even before the famous essay by Warren and Brandeis, i.e., in the period of before the civil war. Westin showed that the name and the privacy content itself were known as much as the jurists who worked before Warren and Brandeis and the judges who had long dealt with cases concerning the use, by third parties, of elements or personal data.

[6] In fact, the term made its first appearance a few years earlier in an essay by Judge Cooley, although with a different meaning. He is talking about the right to be let alone simply wanted to allude to that inseparable part of any right to civil liberty called negative liberty.

[7] On this point, see S. Rodotà, Interview on Privacy and freedom, in P. Conti (ed.), Roma-Bari, 2005, where it states: "The prohibition of entry into the space of others is the cultural junction related to the original story of the concept of privacy, of an area that belongs only to you and to those with whom you want to share it'. It is the right to be left alone. The private life was therefore protected with the logic of the fence."

not because of its public value, in market relations or legal transactions, but because of its owner's value[8].

A further significant contribution in theorizing the concept of Privacy was provided by the jurist William Prosser in an article, "Privacy," published in 1960. The theory of Prosser was based on the rejection of the unitary principle of Privacy - a concept which Warren and Brandeis had instead defended - claiming, on the other hand, a pluralistic conception. The theory of Prosser was not without criticism[9]. He categorized the violation of Privacy into four main categories: the first category was the one regarding the intrusion into the private space, the second condition was about the public disclosure of all private facts concerning a person, the third category is the one about putting a person in a bad light in a public way, and the fourth and last category is the use of someone else's name or personal information without that person's consent[10].

Edward Blounstein published an article in New York City University Law Review a few years later, in 1964, in which he declined to embrace the theoretical elaborations of Prosser, proposing a return to a single vision of Privacy, conceived as an intrinsic value of man and a right worthy of protection in all regulatory areas[11].

---

[8] U. Pagallo, *The protection of Privacy in the United States of America and Europe*, Milan, 2008, pp. 64-65.

[9]. Prosser's theory disregards the existence of a right to Privacy in its own right and, carrying the theme in the field of torts, is concerned to demonstrate that the violation of Privacy does not give rise to a single and new illicit (tort), but can generate four different types of illicit to which correspond three distinct interests. The torts of which Prosser speaks, even if they are assumed under the same denomination, have characteristics significantly different from each other and are united, in the author's opinion, by a single element which is that of representing each one interference with the right to be let alone.

[10] Neil M. Richards and Daniel J. Solove, 2010, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev., 1887.

[11] E. J. Blounstein, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, in New York University Law Review, 1964, page. 974, supports "I contend that the gist of the wrong in the intrusion cases is not the intentional infliction of mental distress but rather ablow to human dignity, an assault on human personality. Eavesdropping and wiretapping, unwanted entry into another's home, maybe the occasion and cause of distress and embarrassment, but that is not what makes these acts of intrusion wrongful. They are wrongful because they are demeaning of individuality, and they are such whether or not they cause emotional trauma".

Meanwhile, in Europe, the exhausting and terrible experience of totalitarian regimes had served as a lesson to understand the imminent importance of Privacy on the other side of the ocean. One of the main elements that were a common denominator between all the various totalitarianism was that they all aimed at alienating the individual, depriving individuals of their freedoms and, consequently, making them embrace the party's ideology. Totalitarianism took away individuals' faculty of choice but comforting them with the propaganda of the dictatorship.[12] Therefore, totalitarian regimes wanted to exercise total control over a person at the expense of his private sphere.

"*Bisogna diffidare dell'argomento di chi sottolinea come il cittadino probo non abbia nulla da temere dalla conoscenza delle informazioni che lo riguardano. L'uomo di vetro è una metafora totalitaria, perché su di essa si basa poi la pretesa dello Stato di conoscere tutto, anche gli aspetti più intimi della vita dei cittadini, trasformando automaticamente in "sospetto" chi chieda salvaguardia della vita privata"*[13].

The idea of "*L'uomo di Vetro*"[14] that nothing must hide, is a metaphor that found its origin in totalitarian regimes based on the concept that countries will know the most intimate aspects of the lives of its citizens. It is crucial to bear in mind that this is still the case nowadays, as stated by Stefano Rodotà, President of the Guarantor Authority for the protection of personal data, in the annual report to Parliament.

Rodotà called for "*adequate attention from the Parliament*," since "*the protection of personal data has become an essential tool for the respect of the principles of dignity and equality"*[15].

[12] Hannah Arendt, 1948, *The origins of Totalitarianism*, Piccola Biblioteca Einaudi

[13] Stefano Rodotà, October 23, 2011, L'ansia di Sicurezza che cancella i diritti, article of La Repubblica.

[14] Stefano Rodotà, October 23, 2011, *L'ansia di Sicurezza che cancella i diritti*, article of La Repubblica

[15] Garante per la Protezione dei Dati personali, 2000, Speech of Stefano Rodotà presenting "annual Report 2000."

1.2 Privacy and Data Protection

We have seen how "Privacy" is a very modern term, and only in the last century has the "right to privacy" become one of our constitutional rights. When talking about "Data Protection," it is essential to remember that it is far more modern and a direct consequence of the "Right to Privacy."

Data security is a right whose value has increased as technological means have progressed and quickly made it possible for all information relating to travel worldwide. Privacy has now become the user's right to have control over information that affects him/her due to the rapid movement of personal data.

Roger Clarke, a consultant who specialized in strategic and policy aspects regarding information infrastructure, data surveillance, and Privacy, in 1997, subdivide the idea of Privacy into four main categories, which were subsequently divided into additional seven categories.

The first four categories were:

1. Privacy of an individual (intended in physical terms), *"Sometimes referred to as 'bodily privacy.' This is concerned with the integrity of the individual's body. Issues include compulsory immunization, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilization*[16]"

2. Privacy concerning human behavior, "*This relates to all aspects of behavior, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as 'media privacy*[17]'"

3. Privacy regarding personal communication, "*Individuals claim an interest in being able to communicate among themselves, using various media, without*

[16]. Roger Clarke, Original of August 15, 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21, 2013, July 24, 2016, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*.

[17] Roger Clarke, Original of August 15, 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21, 2013, July 24, 2016, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*.

routine monitoring of their communications by other persons or organizations. This includes what is sometimes referred to as 'interception privacy[18]*'"*

4. The Privacy of Personal Data, "*Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy*[19]*'".*

The last two aspects, particularly after the 1980s, have become closely linked to the deep association that has taken place between contact and I.T. This is the central theme of the public's attention and this article. It is useful to use the term " Information Privacy" to refer to the combination of contact privacy and data privacy.

A further troubling pattern had emerged around 2005, leading to a fifth dimension that was not evident when Roger Clarke initially structured this in the mid-1990s;

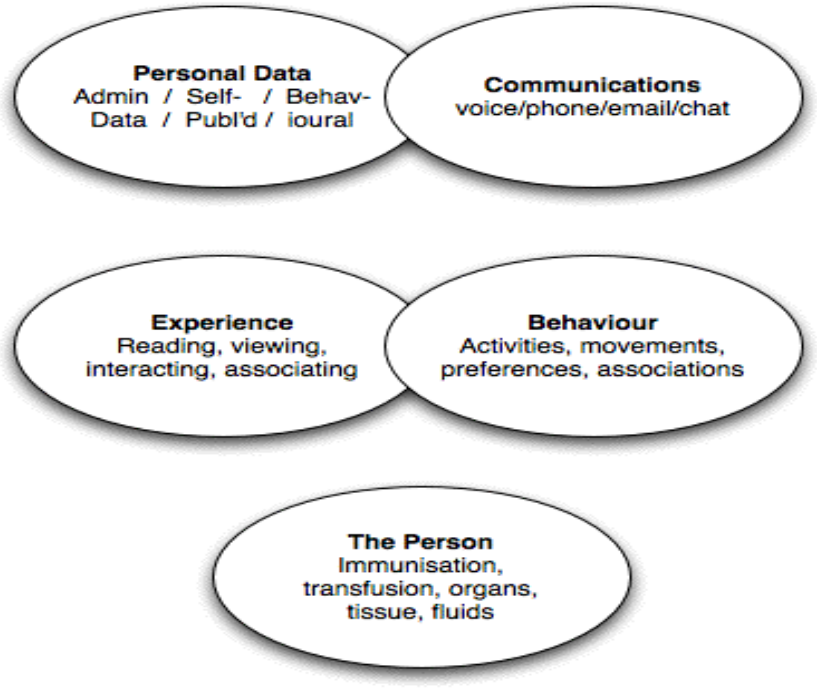
5. Privacy of personal experience of an individual. *"Individuals gather experience through buying books and newspapers and reading the text and images in them, buying or renting a recorded video, conducting conversations with other individuals both in person and on the telephone, meeting people in small groups, and attending live and cinema events with larger numbers of people. Until very recently, all of these were ephemeral, none of them generated records, and hence everyone's small-scale experiences, and their consolidated large-scale experience, were not visible to others. During the first decade of the 21st century, reading and viewing activities have migrated to screens, are performed under the control of corporations, and are recorded; most conversations have become "stored electronic communications," each event is recorded, and both 'call records' and content may be retained; many individuals'*

[18] Roger Clarke, Original of August 15, 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21, 2013, July 24, 2016, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*.

[19] Roger Clarke, Original of August 15 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21 2013, July 24 2016, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*.

locations are tracked, and correlations are performed to find out who is co-located with whom and how often; and events tickets are paid for using identified payment instruments. This massive consolidation of individuals' personal experience is available for exploitation and is exploited[20]*."*

The division of Privacy into four categories elaborated by Roger Clarke can be synthesized as follows:



21

[20] by Roger Clarke, Original of August 15 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21 2013, July 24 2016, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.*

[21] Roger Clarke, Original of August 15 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21 2013, July 24 2016, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.*

As mentioned above, in 2013, Rachel Finn and David Wright divided the categories as mentioned earlier of Clarke into other seven categories:

1. Privacy regarding people "*Encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. According to Mordini, the human body has a strong symbolic dimension as the result of the integration of the physical body and the mind and is "unavoidably invested with cultural values*[22"23]

2. Privacy towards thought and feelings, *"People have a right not to share their thoughts or feelings or to have those thoughts or feeling revealed. Individuals should have the right to think whatever they like. Such creative freedom benefits society because it relates to the balance of power between the state and the individual*[24"25].

3. Privacy concerning location and space, "*Individuals have the right to move about in public or semi-public space without being identified, tracked, or monitored. This conception of Privacy also includes a right to solitude and a right to Privacy in spaces such as the home, the car, or the office. Such a conception of Privacy has social value. When citizens are free to move about public space without fear of identification, monitoring, or tracking, they experience a sense of living in a democracy and experiencing freedom. Both these subjective feelings contribute to a healthy, well-adjusted democracy. Furthermore, they encourage dissent and freedom of assembly, both of which are essential to a healthy democracy*[26"].

4. Privacy of personal data and images, "*includes concerns about making sure that individuals' data is not automatically available to other individuals and organizations and that people can "exercise a substantial degree of control*

---

[22] Emilio Mordini, "*Whole Body Imaging at airport checkpoints: the ethical and political context,*" in Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields, ed. René von Schomberg (Luxembourg: Publications Office of the European Union,2011.

[23] Rachel Finn and David Wright, 2013, *Seven types of privacy* Trilateral Research & Consulting, London Michael Friedewald, Fraunhofer ISI, Karlsruhe

[24] Goold, "Surveillance and the Political Value of Privacy."

[25] Rachel Finn and David Wright, 2013, *Seven types of privacy* Trilateral Research & Consulting, London Michael Friedewald, Fraunhofer ISI, Karlsruhe

[26] Ibidem

over that data and its use"[27]*. Such control over personal data builds self-confidence and enables individuals to feel empowered. Like Privacy of thought and feelings, this aspect of Privacy has social value in that it addresses the balance of power between the state and the person"*[28]*.*

5. Privacy on behavior and actions, "*This concept includes sensitive issues such as sexual preferences and habits, political activities and religious practices. However, the notion of Privacy of personal behavior concerns activities that happen in public space, as well as private space, and Clarke makes a distinction between casual observation of behavior by a few nearby people in a public space with the systematic recording and storage of information about those activities.*[29] *The ability to behave in public, semi-public, or one's private space without having actions monitored or controlled by others contributes to "the development and exercise of autonomy and freedom in thought and action*"[30].

6. Privacy on communications "*Aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone, or wireless communication interception or recording and access to e-mail messages. This right is recognized by many governments through requirements that wiretapping or other communication interception must be overseen by a judicial or other authority. This aspect of privacy benefits individuals and society because it enables and encourages a free discussion of a wide range of views and options and enables growth in the communications sector*[31]*".*

7. Privacy concerning the association "*Is concerned with people's right to associate with whomever they wish, without being monitored. This has long been*

---

[27] Roger Clarke, Original of August 15 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21 2013, July 24 2016, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.*

[28] Rachel Finn and David Wright, 2013, *Seven types of privacy* Trilateral Research & Consulting, London Michael Friedewald, Fraunhofer ISI, Karlsruhe.

[29] Roger Clarke, Original of August 15 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21 2013, July 24 2016, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.*

[30] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford CA: Stanford University Press, 2010).

[31] Finn, Wright, and Friedewald, 2013, *Seven types of Privacy* in S. Gutwirth and others, European Data Protection: Coming of Age, Springer

recognized as desirable (necessary) for a democratic society as it fosters freedom of speech, including political speech, freedom of worship and other forms of association. Society benefits from this aspect of Privacy in that a wide variety of interest groups will be fostered, which may help to ensure that marginalized voices, some of whom will press for more political or economic change, are heard. This aspect of Privacy was not considered by Clarke, and a number of new technologies outlined below could negatively impact upon individuals' Privacy of association[32]".

Thus, we can understand that the concept of Data Protection has long been incorporated into the Right to Privacy. After a long and troubled process of recognition and affirmation, the initial right to be left alone has been transformed, therefore, into the right to the protection of personal data, which, by now, has become a fundamental right of the individual both within the national legal system and within that of the Community[33].

Article 8 of the Charter of Fundamental Rights of the European Union, which was the first international human rights security document to include an ad hoc clause, subsequently obtained and adopted the Directive principles. Indeed, in addition to respecting the more general right to Privacy, the Charter, in Article 8, explicitly and expressly guarantees the right to the protection of personal data, thus granting it complete legal protection autonomy[34].

---

[32] Finn, Wright, and Friedewald, 2013, *Seven types of Privacy* in S. Gutwirth and others, European Data Protection: Coming of Age, Springer

[33] Cfr. S. Rodotà, Introduction, in D. Lyon, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Milano, 2002, page. XI.

[34]. Thus, the right to the protection of personal data is outlined as a new and autonomous right that differs from the right to Privacy. On this point, we refer to S. Rodotà, who underlines "in the right to the respect of private and family life, the individualistic moment is manifested above all, the power is substantially exhausted in excluding interferences of others: the protection is static and negative. Data protection, on the other hand, establishes inescapable rules on the modalities of data processing, it is concretized in powers of intervention: the dynamic protection follows the data in their circulation (...) the protection is no longer only individualistic, but involves a specific public responsibility."

As will be explained in the following chapter, with the European Charter of Human Rights (ECHR) proclamation, Data Protection has been elevated as a fundamental right as much as the Right to Privacy and the Right of Expression is.

The protection of Personal Data means, on the one hand, protection of your Privacy, but on the other hand, it also represents the safeguard of other objectives. For this reason, over time, this right has been recognized as a right in its own right.

It is also essential to bear in mind that protecting Personal Data is based on important ethical and moral values. One of these is undoubtedly the guarantee of human dignity.

The extensive collection of Personal Data, including sensitive data concerning and an individual, could sometimes cause discrimination. Consequently, a right to the protection of personal data becomes necessary to ensure equality.

For example, in Health Data, a right to protection is necessary because the latter would guarantee the right to health. Therefore, the protection of personal data becomes a necessary component in the plurality of individuals' freedoms.

According to two jurists, such as De Hert and Gutwirth, Privacy and Data Protection are two sides of the same coin, two different yet complementary rights. Both jurists point out that the Right to Privacy is a negative right that entails protecting an individual's grey area, therefore a right of non-interference. *"Privacy pre-eminently imposes itself as the legal concept translating the political endeavor to ensure non-interference (or opacity) in individual matters. It is embedded in the current democratic constitutional state, the values of individualism, and the constitutional separation between state and church. It is also intimately linked with the idea that individuals are able and willing to unshackle themselves from tradition, social conventions, or religion and dissociate themselves, up to a point, from their roots and upbringing. Privacy,*

negatively stated, protects individuals against interference in their autonomy by governments and by private actors.[35]"

The right to data security, on the other hand, is committed to demonstrating the ability of those keeping personal data to be transparent. According to De Hert and Gutwirth, in doing so, Privacy must establish security around individuals to guarantee an area of autonomy and independence in which the individual may travel.

"Privacy protects the fundamental political value of a democratic the constitutional state as it guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards - for example - their sexuality, health, personality building, social appearance and behavior, and so on. It guarantees each person's uniqueness, including alternative behavior and the resistance to power at a time when it clashes with other interests or with the public interest[36]*."*

On the other hand, in protecting personal data, it is necessary to focus on the transparency of those who hold the data[37].

The right to Privacy was created with two characteristics: proportionality and consensus. As for what concerns the collection of personal data, it must always require the individual's consent. The use of these data must be proportional to the purpose for which they were collected initially. The data

[35] Such a negative understanding of Privacy can clearly be read in Article 8 ECHR's formulation: no interference by public authorities is permitted unless necessary in a democratic society.
[36] De Hert P. & S. Gutwirth, 'Privacy, data protection, and law enforcement. The opacity of the individual and transparency of power' in E. Claes, A. Duff & S. Gutwirth (eds..), Privacy and the criminal law, A. About this concept of Privacy, see a.o. S. Gutwirth, Privacy and the information age, o.c., passim and S. Gutwirth, Privacy's freedom: a condition for social diversity, A.M.P. Gaakeer & M.A. Loth (Red), SI-EUR Reeks 28 , Arnhem, Kluwer/Gouda Quint, 2002, 95-138
[37] De Hert and Gutwirth, 2009, *Data Protection in the Case of Law of Strasbourg and Luxemburg: Constitutionalisation,* Springer.

collected, therefore, which will be manipulated may be used only for the purpose for which they were collected initially.

Several jurists, however, pointed out boundaries to these essential points. Bygrave and Schartum point out that a formal, free, and sometimes inevitable act is consent.
Proportionality, on the other hand, is not a criterion that is minimal enough. The alternative proposal is a shared exercise of consent that would reinforce the individual's status concerning those keeping the data.

1.3 Digital era: End of Privacy?

"*Technological advances had allowed personal information to be collected, stored, analyzed, copied and distributed with ease and level of sophistication that would have been unimaginable when the data protection and privacy acts were passed*[38]".

Privacy is an essential and fundamental right of democracy, which at the same time, constitutes a guarantee of the security of other freedoms. Nevertheless, the introduction of emerging digital technology is one of the biggest challenges that the Right to Privacy must face.
The technological and telematics revolutions have had profound consequences for the World of law. In some cases, the law has attempted to use existing rules without adapting to the novelty of the technology; in others, it has "abdicated" its regulation, leaving to technology the task of giving the rule to the concrete case[39].

[38] Burrows, 2011
[39] See the contribution of G. Pellegrino, I rischi del diritto nella Rete globale, in Informatica dir, 2009, fasc. 1, 256.

It was only later that legislation restored its regulatory role and continued to monitor the various phenomena that were always new and increasingly difficult to deal with.

All of this has undoubtedly influenced the system of sources on the law's certainty and effectiveness, which is no longer solely related to the state's character, and therefore to the basic concept of legality.

In concrete terms, the legal reality has changed, and with it, the conceptions of conceptions of space[40], property[41], document[42], contract[43], freedom[44]And others.

Privacy and data security are concepts that affect all nowadays. We are aware that by profiling its consumers to enforce their marketing plan, the company uses our personal data for commercial purposes. Similarly, governments are adopting new monitoring policies in order to collect more information about their citizens, announcing it in the name of public and national security.

It is of growing importance the issue of information security that concerns both private citizens and companies, involving all aspects concerning the protection

[40] A careful analysis can be found in V. De Rosa, The formation of legal rules for The "Cyberspace," in Dir. information and computer science, 2003, fasc. 2, 361-362: "With the development of the "Information Technology" a new space has come to be created, or, if one prefers, a new spatial dimension in which human activity is to be carried out in all its manifestations and with respect to which the computer medium constitutes an organon, that is to say, an instrument of perception and, at the same time, of creation of the same space; constituted by the interactions that are established between the artificial intelligences created by computer systems (whose study is the specific object of the systems (the study of which is the specific subject of cybernetics) as well as the relationships that are to be established within it: what is usually called cyberspace."

[41] See as an example of a new proprietary paradigm, S. Montaldo, Internet and Commons: network resources in the perspective of the commons, in Dir. information and computer science, 2013, fasc.2, 287-306.

[42] On the digital document is exhaustive in the chapter devoted to it G. Pascuzzi, The law of the digital era Il Mulino, Bologna, 2010, 98-122. In the new edition of the work of 2016 the second chapter, written by Giovanni Pascuzzi and Paolo Guarda, is dedicated to the evolution of the concept of document and subscription: G. Pascuzzi (ed.), Il diritto dell'era Digitale, Il Mulino, Bologna, 2016, 77-94

[43] See two interesting contributions on contracts concluded via the Internet, C. Rossello, Commercio Elettronico: la governance di internet tra diritto statuale, autodisciplina, soft law e lex mercatoria, Giuffrè, Milano, 2006; G. Finocchiaro, Lex mercatoria e commercio elettronico, the law applicable to contracts concluded on the Internet, in Contr. impr., 2001, fasc. 2, 573: "the problem of the identification of the law applicable to acts performed via the Internet is a problem of general character, and is indeed the problem of greater importance that, among the issues raised by the great network, is posed today to the jurist."

[44] See, for a reflection on the new freedoms, including political ones, M. Cuniberti, Tecnologie digitali e libertà politiche, in Dir. informazione informatica, 2015, fasc. 2, 275-314.

of sensitive data stored digitally and in a particular way is known to the general public because of the use of the Internet.
The extensive network can offer a wide range of information and services. However, at the same time, it can be a dangerous place for our Privacy also because the medium itself is not designed to exchange or manage sensitive data.

The progressive development of electronic communications has determined the exponential growth of new services and technologies. While this has led, on the one hand, to unquestionable advantages in terms of simplification and speed in the retrieval and exchange of information between internet users, on the other, it has caused a considerable increase in the number and types of personal data transmitted and exchanged, as well as the dangers associated with their illicit use by unauthorized third parties.
The need to ensure robust protection of people's rights and freedoms, concerning individuals' personal identity and private life using telematic networks, has thus become more widespread[45].

The development of modern technologies and new electronic communication services makes it necessary to adapt further the regulations on protecting personal data in Italy and internationally. Moreover, this aspect has been considered in the issuing of European Regulation on the protection of personal data.
Of course, the risk of disseminating electronic records such as electronic cards, the emergence of authentication and identification services as SPID, and the interconnection of the computerized archives remain and may lead to a reduction of personal rights and confidentiality of personal data.
The same Guarantor Authority for the protection of personal data, in the exercise of the advisory function of which it is owner, has repeatedly reported, in previous years, the need to identify with greater attention and proportionality the type of

[45] O. Zangrilli, "Open Government: dalla Semplificazione della P.A. alla e-Democracy," 2018

data to be included in electronic documents. These subjects can possibly access the various categories of data and the guarantees for those concerned[46].
In fact, in today's technological age, an individual's personal characteristics can be easily split up and merged into different databases, each of them with a specific purpose. On this assumption, the so-called electronic person, corresponding to our digital identity, can be easily reconstructed through the many traces the person leaves in the computers that record and collect information about him.

One must always remember that new technologies' objective is to improve citizens' quality of life while respecting security and Privacy. Any problem concerning the relationship between new technologies and Privacy must always be solved by framing it within a global consideration of socio-economic benefits that arise from technological innovation. For example, the significant advantages represented by the database present on the Net cannot be overlooked in the performance of the administrative activity and the general improvement of the quality of life of citizens and the promotion of productive and economic activities[47].

We understand that our Code's approach to protecting personal data is "technologically neutral." However, the Guarantor Authority itself intervenes with its own general measures to make up for the legislation's inevitable shortcomings.
Therefore, it is neutral that in this evolutionary framework, not always ideal, the Guarantor for the protection of personal data in the face of the development of new technologies maintains a conservative attitude, studying the main implications of each new device or service distinguished by its novelty.

Typically, even before issuing general measures or guidelines, public consultations are promoted, as in the recent case of the Internet of Things (IoT),

[46] O. Zangrilli, "Open Government: dalla Semplificazione della P.A. alla e- Democracy," 2018
[47] Ibidem

in order to have a complete general picture about the usefulness and opportunity of that particular device or service.

"Le derive tecnologiche possono produrre gravi effetti distorsivi. E questa perché la protezione dei dati personali rischia ogni giorno d'essere compromessa dalla crescente offerta sul mercato di tecnologie che rendono più agevoli forme generalizzate di raccolta delle informazioni"[48].

We may remember that Rodotà himself spoke of technological drift to indicate the phenomenon of a growing and not always fair chase to continuous progress of technological nature.
We are now close to a change that can be defined as epochal, for our society, with the advent of the European Regulation on the protection of personal data wanted precisely because of the new dimension that the privacy problem has taken on with technological progress.
The transnational nature in a global sense of Internet with all public and private applications, web sites generalist, social networks, financial e-commerce applications, digital marketing platforms, and communication, require rigorous privacy and security policies to prevent and avoid the serious risks involved in the possible theft of digital identity, unauthorized profiling and fraud in general.

The Internet must be considered the most potent vehicle of data dissemination, and therefore technically, the potentially most dangerous in terms of breaching the confidentiality aspect. The Italian Authority put in the control of privacy issues in the hands of the Privacy Guarantor, which in addition to overseeing abuse by issuing stringent guidelines and policies to try to minimize violations[49].

When talking about Open Government and simple access to public data, for example, special attention should be put on the control of the

[48] Stefano Rodotà, *Annual Privacy Report*, 2004
[49] O. Zangrilli, "Open Government: dalla Semplificazione della P.A. alla e- Democracy," 2018

"interoperability" of the systems, which technically would allow, in addition to the possession of information concerning absolutely confidential citizens and businesses, the "construction" of fictitious profiles, and theoretically fake digital identity cards, health cards used for fraud or manipulation in the broadest sense. If, on the one hand, CAD pushes for the opening and the simplification of access to public database, even in the distinction between data "knowable" by anyone, and data "a limited knowability", on the other hand the guarantor of privacy has the need to regulate in a strict way the construction itself of public database, which in the case of personal information on citizens and businesses must for of all, *"assicurare l'esattezza delle informazioni, l'aggiornamento, la pertinenza e non eccedenza dei dati, e garantire il rispetto del diritto all'oblio quando le informazioni raccolte esauriscono il loro scopo*"[50]

A subject as complex as the Protection of Personal Data and Sensitive Data, especially if transplanted on a powerful medium such as the Internet, has imposed over the years coordination between the various States, and for what concerns us especially within the E.U., which although inspired by interests and common security, has very often been the subject of interpretation by the individual States such that the application of the standards has been very "variable."

To overcome this situation, to respond to the new technological challenges, and above all, to harmonize policies within the E.U., on May 26, 2018, the "Reform of the E.U. Data Protection rules," E.U. regulation N.2016/679, better known as the GDPR (General Data Protection Regulation) came into force.

From 2016 until its entry into force, this regulation has been subject of in-depth analysis by strategic direction with the DPIA (Data Protection Impact Assessment) protocol, which in consideration of the continuous evolution of technological devices, artificial intelligence, machine learning, up to I.o.T (Internet of things) outlines three fundamental guidelines concerning the timing of the risk analysis, to the determination of treatment of individual-specific areas, and concerning the "device" component used on the technological plan. The

[50] GarantePrivacy.it

elements of substantial modification of the GDPR compared to the previous regulations are the following:

1. *Accountability of the Owner*, i.e., it is a very extended responsibility and its measurability.
2. *Privacy by Design*, i.e., considering the confidentiality and protection of data from the Design of any sensitive process.
3. *Treatment Register*.
4. *Risk Assessment* (Data Protection Assessment), i.e., general impact assessment.
5. *Adoption of appropriate technical and organizational measures*
6. *Data breach*, communication of any data breaches within 72 hours to the competent Authorities.
7. *Certification of treatments*, compliance with the Regulations through certification mechanisms
8. *Duration of the treatment*; new timing of data retention.
9. *Data Protection Officer (DPO)* established a new mandatory position in all private and public organizations.
10. *Joint and several liabilities of owner and manager.*
11. *The magnitude of the sanctions*, with tightening of sanctions.

Another aspect of particular importance in the progressive "digitization" of the World is that of computer security, necessary to protect the citizen not only within his sphere private, but especially in terms of civil society as a whole, and in its expressions of democracy[51].

The manipulation of personal data and the possible hacking of the public networks represent one of the factors of greater risk in the Internet world. The counter-measures possible adopted are constantly being overtaken by new data breach systems, from simple phishing of the private computers to potential, and sometimes implemented, possibilities of infiltration into government systems, capable of undermining the very integrity of the processes of expression of democracy.

[51] O. Zangrilli, "Open Government: dalla Semplificazione della P.A. alla e- Democracy," 2018

In this sense, two are emblematic recent events that force cybersecurity experts to reconsider current defense protocols.
In the Netherlands, the general elections in 2017 were characterized by the government's decision to count the votes "by hand" to avoid the possibility of hacking, putting aside the electronic counting system that is only just old.
Eight years old.
This decision, to avoid the risk of interference and potential manipulation by Russia, such as declared by the outgoing government, undoubtedly derives from the scandal of the 2016 U.S. presidential election, where to the suspicions of cyber-interference in the elections by Russia, which would have, according to the thesis still object of investigation, manipulated the data to facilitate Trump's election, followed the Cambridge scandal Analytica, which through the violation of more than 50 million Facebook profiles, would have strongly influenced not only the American elections, always in favor of Trump, but also those of the United Kingdom pro-Brexit.

The accusation towards comparisons of the Cambridge Analytica company is to have used algorithms based on Facebook data for to package high level "fake news," able to modify the perception of reality by the subjects, and therefore condition its behavior, also in the field of political choice. Therefore, the cyber-crime is intertwined with the fundamental processes of democracy and can represent a tremendous potential risk for all countries.

In the European Community, Internet protection is considered an indispensable strategic factor for the integrity of national sovereignty and democracies and a factor of growth protection digital economy.

The "Strategy for the E.U. Digital Single Market" is given a contribution value economic growth of more than 400 billion per year in economic exchanges, job creation, and transformation of economies. Therefore, the protection of the Internet is an absolute priority, both political than economic. The E.U. Cyber Security Strategy of 2013, with the updates introduced in 2017,

requires everyone to the Member States to adopt a cybersecurity strategy. As is often the case with implementations of the European Union policies are very variable in the various States.
The models of excellence and best practices more advanced are those of the U.K., which, starting from massive investments in university research and the sector companies, have pursued becoming the "safest" place to conduct business online. Today, thanks to huge investments, the National Cyber Security Centre, the national authority responsible for cybersecurity, also coordinates international collaboration and export activities. From an economic point of view, the English model with the organizational architectures field of prevention and contrast.

Speaking of the Internet, of Cyberspace, of World Computer Wars, has limited value to analyze national cybersecurity implementations. While you probably cannot expect large multinational companies in the future, always fighting among themselves for the conquest of market space and customers, can be the driving force of a world safer Internet, there will be an increasing need for coordination actions between governments around the WorldWorld, with the exchange of experiences and the most advanced organizational models, through homogeneous legislation, and especially with the presumption that they work for peace and security, to cope with that which must be considered not only a threat but today also a real "global" emergency.

Chapter 2: European Framework on Data Protection

2.1 . E.U. as the leading promoter of the "Right to Privacy": Evolution of the ECHR and the evolution of Art.8 within the Jurisprudence of the ECHR

Today, the collection of personal data[52] is one of the main features of the 40th European legal system, which attributes to the right to privacy, considered inviolable, the same meaning of basic human rights.

Initially, the Community legal system, formulated from an economic incorporation point of view, did not recognize the issue of privacy regulation by specific legal provisions, because privacy is a matter of general interest t a matter of human rights. However, through the jurisprudence of the courts[53], Europe has also taken measures to defend the basic principles of the individual (and, with them, privacy).

The evolutionary process and the subsequent legal recognition of the right to privacy, as an independent condition worthy of protection, has also found several complications in our continent, as evidenced by the American experience.

There is no doubt that in the first half of the nineteenth century, the tragic experiences of authoritarian regimes established and reinforced in the European mentality the importance that must be assigned to the security of the private spheres of the people. After living through a dark time in which

[52] Data processing means "any operation, carried out even without the aid of electronic instruments, concerning the collection, registration, organization, storage, processing, use of personal data and the processing of personal data electronic instruments, concerning the collection, recording, organization, storage, consultation, processing, modification, selection, extraction, comparison, use, disclosure and use of data consultation, elaboration, modification, selection, extraction, comparison, use, interconnection, blocking, communication, dissemination, cancellation of data, even if not recorded in a database." On the notion of data processing, see L. Lambo, *The discipline on the treatment of the personal data: exegetical and comparative profiles of the definitions*, in R. Pardolesi (edited by), Diritto alla riservatezza e circolazione dei dati personali,cit., pg. 75.

[53] Reference is made to the European Court of Human Rights and to the Court of Justice of the European Union.

the everyday life for millions of people was censorship, racist laws and other oppressive measures, the need was felt everywhere to protect the person and his freedoms and could be replicated in history to avoid similar horrors and disasters.

The European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950, is usually traced back to the first normative references to privacy[54].

The necessary work of the Council of Europe, a regional body with a universal vocation, born in the ashes of the Second World War, was at first the catalyst for the promotion of the right to privacy[55]. The Organization of Strasbourg, established in 1949 with the gradual adhesion of the new democracies of the countries of Eastern Europe, has now acquired a pan-European dimension, currently comprising 47 states. The Council of Europe's purpose is to promote the values which constitute the shared heritage of the Member States: democracy, the rule of law and respect for human rights, the latter of which are secured by the most relevant conventions of the Council: The European Convention on Human Rights and Fundamental Freedoms for the Protection of Human Rights. The latter is covered by the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, the most relevant convention of the Council.

[54] The Council of Europe, the world's leading human rights organization, has a total of 47 member states, including the 28 members of the European Union. All the member
States are signatories to the ECHR, a treaty designed to guarantee the protection of human rights, democracy, and the rule of law. The body responsible for controlling the implementation of the of the ECHR within the member states is the European Court of Human Rights in Strasbourg. The website of the Council of Europe can be consulted at www.coe.int.

[55] The European Convention for the Protection of Human Rights and Fundamental Freedoms was signed in Rome on November 4, 1950 and entered into force on September 3, 1953 following the deposit of at least 10 instruments of ratification. For Italy it came into force only from October 10, 1955 following the ratification with the law n.848 of August 4, 1955, and subsequent publication in the Official Gazette n.221 of September 24, 1955. Today all 47 member countries of the European Council are part of the treaty.

The ECHR is the first treaty aimed at the security of individuals and, to this day, the only treaty with a permanent guarantee system within the jurisdiction to which any person may qualify for the protection of the rights guaranteed by the Convention.

Article 8 on the right to protect personal and family life is especially important to the subject matter discussed here:

> *"1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui."*[56]

Article 8 is primarily meant to protect people from public authorities' unreasonable intervention. State Parties are forbidden from interfering, unless explicitly prohibited exemptions.

In this respect, intervention may be provided for by statute or may be driven by one of the general imperative conditions referred to in the second paragraph of Art. 8. positive obligations to take action to ensure effective respect for "family life" complement the pledge of negative character of the States Parties. Effective respect for "family life and private life" shall be assured. The boundary between the Contracting States' positive and negative obligations under Article 8 is not precisely defined, but the principles in force are comparable. In meeting all responsibilities (positive and negative), the State must find a reasonable balance

[56] Convention for the Protection of Human Rights and Fundamental Freedoms Concluded in Rome on 4 November 1950, Approved by the Federal Assembly on 3 October 19742 Instrument of ratification deposited by Switzerland on 28 November 1974, Entry into force for Switzerland on 28 November 1974.

between the competing interests of the public and of individuals. Furthermore, the decision-making process envisaged must be "just" and ensure that the interests covered by Article 8 are properly respected[57].
In particular, *"The principle of proportionality must exist between the [challenged] measure and the purpose pursued*"[58].

The increased amount of information in circulation brought the issue of personal data security to the fore as automated data processing became more prevalent, further changing the nature of the confidentiality of an individual and the definition of privacy. This is the basis on which more personal data security treaties have subsequently emerged.

The concept of "private life" established by the Strasbourg Court's jurisprudence is a general concept and is not subject to an exhaustive definition. Not subject to an exhaustive description that requires the individual's physical and moral integrity and can, thus, include certain facets of an individual's identity.
The right to respect "private life" means that each entity can, in essence, create his or her own personal life identification.

[57] Judgment of June 3, 2014, sec. 3, Lopez Guiò v. Slovakia
[58] In its judgment of 3 October 2014, the Grand Chamber of the Strasbourg Court, Jeunesse v. Netherlands, on the issue of Jeunesse v. Netherlands,
Immigration held that there was a breach of Article 8 in a situation where, despite the presence of extraordinary circumstances, the Netherlands had declined to issue a residency permit for family reasons. The Court found that there was no compromise between the applicant's personal interests, which were those of a Surinamese national who had entered the Netherlands, and those of her personal interests. A Surinamese citizen who had entered the Netherlands on an expired tourist visa and was married to a Dutch citizen with whom she had three children and who had applied for a family residence permit. Italian legislation declined to give a social security contribution to a non-EU resident in possession of a standard work permit and a residency permit, EDU Court, March 27, 1998, Petrovic v. Austria, in part. § 26; EDU Court, July 9, 2009, Zeïbek v. Greece, in part part. § 32; EDU Court, 28 October 2010, Fawsie v. Greece, in part. § 27); in the same sense of the violation of Article 8, the judgment of December 4, 2012, second section, Hamidovic v. Italy, whereby the interference of the States Immigration steps can be made up of members of the private and family life covered by Article 8. The Edu Court found in the present case that the expulsion measure was not proportionate to the purpose sought. Security defense in a democratic society, which results in a violation of Article 8 of the Convention.

The identity of a person includes many facets and is composed of many components. Among the many aspects of the identity of a person are the name[59] or the elements connected with the right to the image[60].
The definition of "private life" often involves personal information that can reasonably be expected by an individual not to be released without his or her permission[61].

The definition of privacy can also be found in the Universal Declaration of Human Rights of 1948, always in general terms, where Article 12 (from which Article 18 of the ECHR derives) summarily specifies a prohibition of "*interference in private life*"[62].
However, a particular provision devoted to the processing of personal data and the regulation of privacy is not included in the Convention.

Nonetheless, the jurisprudence of the Strasbourg Court *"has introduced in Article 8 a detailed understanding of the "private life" formula, specifying in several Statements the applicability of its protections even regarding the processing and storage of personal data*[63]", making a decisive contribution to the "positivity" of the right to privacy.

In 1981, "*Convention No. 108 for the Protection of Persons with respect to the Automated Processing of Personal Data*" was promoted for this reason, following in the footsteps of international judges' pronouncements in the field of human rights, influenced primarily by Article 8 of the ECHR. The implementation of the concept of 'equivalent' protection, according to which the

[59] Judgment of December 5, 2013, V sez., Henry Kismoun v. France, on the subject of changing the surname and first name of natural persons.
[60] Judgment of February 7, 2012, Grand Chamber, Von Hannover v. Germany, n. 95-96.
[61] Judgment of 6 April 2010, IV sez., FLinkkila and Others v. Finland,n.75
[62] In fact, the matter will be more accurately regulated by the Council of Europe Convention of 43, 28 January 1981, concerning the protection of persons with regard to automatic processing of personal data, and the subsequent Nice Charter, which is considered of fundamental importance for the "Constitutionalisation" of the right to privacy.
[63] F. Cardarelli, S. Sica, V. Zeno-Zencovich, The personal data code. Themes and 44 problems, Giuffrè, Milan, 2004, cit. Giorgio Resta, Il diritto alla protezione dei dati personali, p. 35.

transfer of personal data between the two States Parties to the Convention[64] may take place only if the legal system of the State receiving the information grants the same guarantees of protection as that of the State sending[65] it, is worth noting among the various creative aspects of the Convention.
The State shall have the same protections of security as those which the sender State has adopted.

However, the formal consecration of human rights in the legislative texts of the European Union, with the subsequent regulation of the right to privacy, was possible only because of the birth of the European Union, sanctioned by the Maastricht Treaty in 1993.

The first discipline, which is symbolically the most relevant[66], is contained in Article 8 of the Charter of Fundamental Rights of the European Union, which guarantees the right of each citizen to the security of his or her personal data, defines procedures and limits of care, and provides for the formation of an independent monitoring[67] authority.

---

[64] The Convention introduces principles regarding the correctness and lawfulness of data collection and automated processing, as well as the quality of data. The Convention introduces principles regarding both the correctness and lawfulness of the collection and automated processing of data, and the quality of such data. The preamble states the The preamble states the principle that the free movement of information cannot disregard the protection of fundamental rights and freedoms. The preamble states the principle that the free flow of information must be accompanied by the protection of fundamental rights and freedoms. processing must be legitimate and the data, accurate and up-to-date, must be processed in accordance with the requirements of the law. Another fundamental principle is that which prohibits the automatic processing of certain types of sensitive data under Article 6, a prohibition that may be waived provided that "domestic law provides appropriate safeguards", i.e. provides for appropriate safeguards", i.e. that the processing of sensitive data are contained and This prohibition can be waived provided that "domestic law provides appropriate safeguards", i.e. that the processing of sensitive data are contained and controlled by appropriate means (so-called principle of "equivalent" protection). There are There are principles relating to the "security measures" to be taken to prevent inappropriate or unauthorized access to data (the principle of adequate or unauthorized (principle of accuracy, proportionality, adequacy).
[65] The European Union would later reformulate this concept in the first Directive 46 issued on the processing of personal data.
[66] Cfr. F. Cardarelli, S. Sica, V. Zeno-Zencovich, op. cit., p. 6
[67] Signed on 7 December 2000, Article 8 of the Charter of Fundamental Rights of the European Union reads as follows: "1. Everybody has the right to the privacy of personal data.
2. Such data shall be reasonably processed for defined purposes and based on the consent of the individual concerned or on any other valid basis provided for by legislation. Law. Every person has the right of access to and rectification of the data collected relating to him or her, 3. Compliance with these laws is subject to an impartial authority's oversight.

If an entity considers the idea of privacy as a right to which a legal guarantee must be reserved, the term "*data protection*" is disseminated, translating the initial right to privacy into a concrete data regulation. Directive 95/46/EC of the European Parliament and of the Council (hereinafter referred to as the *"Data Security Directive*" or the "*Mother' Directive*") marks the beginning of the long and troubled legal development of the processing of *personal data* in Europe[68].

Thus, in addition to offering an adequate description of *personal data*[69], the European legislator accepts the current profile assumed by privacy with a view to preserving the rights and freedoms of individuals regarding the collection of personal data and the free flow of personal data and sets out concepts relating to their validity.

The main purpose of the Directive is to define a compromise between respect for the right to privacy and the free flow of personal data within the Member States, so that the economic interests on which the European Union[70] is centered do not clash with the fundamental values of a person's personality.

Indeed, the Court of Justice of the European Union has intervened on many occasions in this regard, acknowledging the protection of human rights (and, subsequently, of privacy) as an integral part of the Community order. Therefore, to meet the two conflicting needs, the Directive lays down a common norm for

[68] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. protection of individuals with regard to the processing of personal data and the free movement of such data, in movement of such data, in G.U.C.E. n. L.281 of 23 November 1995, was followed by Directive n. 97/66/EC of December 15, 1997, regarding the protection of personal data and the protection of privacy in the telecommunications sector, which was subsequently repealed in the telecommunications sector, subsequently repealed and replaced by Directive no. 2002/58/EC of July 12, 2002, regarding the protection of personal data and privacy. EC of July 12, 2002 concerning the processing and protection of personal data and privacy in the electronic communications sector. in the electronic communications sector.

[69] Art. 2(a) of Directive 95/46/EC defines personal data as "any information concerning an identified or identifiable natural person ('data subject')" concerning an identified or identifiable natural person ("data subject"); an identifiable person is one who can be
identifiable person" means a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

[70] It should be recalled that the EEC, i.e. the European Economic Community, was formed as the EU, with the goal of establishing a single market focused on the free movement of citizens, goods, services and capital. The Community legal framework is therefore also concentrating on economic integration.

the protection of fundamental human rights which Member States are expected to uphold.

In relation to previous interventions on the subject, the creative aspect consists of putting the user and his private life[71] at the center of personal data processing activities.

It defines, in general, the right of the data subject to obtain information on the processing of the data, as well as the right of access to the data, with the possibility of rectification, cancellation and freezing of the data subject, or even the right to object to the processing.

In order to completely guarantee the defense of the fundamental rights of individuals, the Directive not only applies a set of standards, rules and security measures to the processing of personal data to which the States must conform, but also creates a special supervisory authority to ensure the proper implementation of the legislation to which the authority has the power to bring legal action against possible violations of the provisions.

The European legislator's objective is clearly to define the center of the laws, principles and common standards aimed at ensuring the homogeneous protection of the personal data of all EU citizens, with a view to "*making the level of protection of the rights and freedoms of individuals equal in all Member States, with respect to the level of protection of the rights and freedoms of individuals of all Member States*[72]*".*

[71] This aspect should not be underestimated as it constitutes the main difference in terms of processing of personal data between the EU and US approaches. The US approach emphasizes the economic and commercial value of personal data, the processing of which is generally permitted. processing is generally permitted. In contrast, under EU law, the processing of personal data is prohibited if it does not have an economic and commercial value. On the contrary, under EU law, the processing of personal data is prohibited unless it has a solid legal basis (ref. art. 7 and 8 of Directive 95/46/EC). It should also be added that the legislation in the United States refrains from imposing restrictions privacy restrictions on the transfer of personal data to other countries and the surveillance mechanisms are much weaker than the mechanisms are much weaker than those in place in Europe. There is no data protection regulator with similar functions and powers to European regulators. similar functions and powers to European authorities.

[72] CJEU, Joined Cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Credito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011, paragraphs 28 and 29. "[...] The approximation of the national legislations applicable in this field must not have the effect of weakening the protection ensured by them, but must, on the contrary, aim at ensuring a high

However, as the Directive was adopted but not completely implemented, the findings obtained were not entirely positive: the required legislative harmonization between Member States proved to be unsuccessful due to the lack of uniformity in the manner in which Member States have adapted the Directive.

Despite the successive changes made to the "*Mother Directive*[73]" to counter the new dangers arising from the growing growth of electronic communications services, which threaten privacy protection and endanger the protection of individual privacy communications services, which threaten privacy protection and seriously jeopardize the security of personal data; a high degree of security does not seem to be assured by the regulation of confidential data, the regulation of the data subject's right of access and, above all, the regulation of data transfer to third countries[74] security degree.
In addition, it is well recognized that the topic of personal data is especially changeable; thus, its discipline needs constant adaptation in the light of technical and social developments[75].

degree of protection in the Community. […] The harmonization of the a forementioned national legislations is therefore not limited to a minimum harmonization but results in a high level of protection in the Community. The harmonization of these national legislations is therefore not limited to a minimum harmonization, but leads to a harmonization which, in principle, is complete".

[73] Directive 2002/58/EC on the processing of personal data and the protection of privacy 54 of the electronic communications sector will subsequently amend the so-called 'data preservation' directive (Directive 2006/24/EC) on the retention of personal data, which, in turn, was invalidated in April 2014 by a decision of the Court of Justice.

[74] As far as the transfer of data to third countries is concerned, this is a subject that deserves separate treatment. The level of protection granted by the European legal system, based on Directive 95/46/EC and 95/46/EC and Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of the framework decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, has undergone significant changes, especially in the last year. considerable especially in the last year, in particular since last October 2015, when the Court of Justice of the European Union decided to invalidate, through the famous "Schrems" judgment, the so-called Safe Harbor (a trade agreement that allowed American companies to store huge amounts of European citizens' data). After lengthy negotiations, the European Union has recently concluded a new agreement with the United States, called "EU-US Privacy Shield" to replace the previous the previous "Safe Harbor".

[75] F. Cardarelli, S. Sica, V. Zeno-Zencovich, op. cit., p. 9.

2.2. Strasbourg Convention n.108

"... Estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, e in particolare il diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica…[76]*"*

In 1981, within the Council of Europe, another significant step forward was taken. That year, the work which led to the opening of the Strasbourg Convention 108 on the Protection of Individuals regarding the Automatic Processing of Personal Data ("Convention 108")[77], a legally binding international treaty on the protection of personal data.

For the 47 member states of the Council of Europe, the Convention has entered into force and Mauritius and Uruguay have also been ratified and entered into force, with Cape Verde, Morocco, Senegal, and Tunisia scheduled to join in the immediate future. Therefore, it cannot be considered that the influence of customary law has yet to be achieved.
This treaty aims, first, to ensure the security of the processing of personal data. The collection of data relating to ethnic origin, political views, religious or other convictions, health or sex life is also forbidden crime convictions and sexual life.

Individuals are assured the right to know what information about them is kept. In relation to a superior concern such as national security or the defense of order, the only downside of any of this is that. Finally, in countries where the standard of security is insufficient, cross-border data flows are reduced.

[76] Preamble Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981
[77] Convention No. 108, signed in Strasbourg on 28 January 1981, on the privacy of persons with respect to the automated processing of personal data signed on January 28, 1981 in Strasbourg. Entered into force following five ratifications on 1 October 1985. Following its signature on 2 February 1983 of Convention 108, Italy deposited its instruments of ratification only on 29 March 1997 and thus entered into force on 1 July 1997.

The Strasbourg Convention imposes minimum rules on the adhering states, leaving them free to follow more comprehensive rules of implementation. For this purpose, countries are often called upon to take protective measures to avoid forms of destruction and unintentional loss of recorded data, and to prevent unauthorized access to and distribution thereof, in any case[78].

Where information is stored in databases, the Convention grants data subjects the right to be informed of the nature and purposes of electronic collection, as well as of the name, registered office, or residence of the data subject.

Data participants also have the right to have unlawfully processed data corrected and removed[79]. In the case of an infringement, recognition of these rights means the right to appeal to the competent authorities[80].

The Data Convention also provides that, under the international agreement, states can nonetheless suspend both obligations and privileges. The domestic law of the acceding country can provide for exceptions to the provisions of the Treaty on grounds relating to public security, state security, monetary interests, the suppression of crime and the preservation of the rights and freedoms of individuals[81].

The goal of harmonizing the laws of the adhering countries correlates with the purpose sought by the Agreement of implementing a region of free circulation of data between them. For this purpose, the flow of information is prohibited or subject to authorization.

On the other hand, if they do not have sufficient assurances of security, transfer of personal data to third countries could not be allowed[82].

[78] See art. 7 Strasbourg Convention
[79] See art. 8 Strasbourg Convention
[80] See art. 8 lett. d) Strasbourg Convention
[81] See Art. 9 of the Convention of Strasbourg. Indeed, in the second paragraph of Article 8 of the C.E.D.U., the existence of exceptions enabling the State to intervene in the private life of individuals was already contained.
[82] See art. 12 Strasbourg Convention

On November 8, 2001, the Strasbourg Convention was amended. A Supplementary Protocol was opened for signature and entered into force on 1 July 2004.

Accordingly, the Agreement has been enriched by clauses containing, on the one hand, the possibility of moving data to third countries and, on the other hand, the duty to set up a supervisory authority called upon to ensure conformity with the legislation adopted for the performance of the obligations under the Convention itself. These last two elements, which are governed by the Convention by an additional protocol, are already included in the Community regulations, which have since been adopted.

The Community has pursued the course of incremental recognition of the right to privacy by the European Council and the jurisprudence of the European Court of Human Rights by the actions of the Court of Justice[83] and the provisions of Art. 6 T.U.E.

The security of privacy and the processing of personal data are an expression of the individual's fundamental right to privacy, an expression of the genetic heritage of European architecture as a "*community of law*"[84].

Indeed, the ideals of equality, democracy, respect for human rights and the rule of law are the founding values of the Union: "*diritto fondamentali quali*

[83] The European Court of Justice, with the Court of First Instance, ensures, in accordance with Art. 220 TEC, respect for the law in the interpretation and application of the Treaties. It is an institution of the European Communities composed of one judge per Member State (Art. 221 The judges are assisted by eight Advocates General, who are called upon to present, with complete impartiality, the case law of the Court of Justice. The judges are assisted by eight Advocates General, who are called upon to present publicly, with absolute impartiality and full independence, reasoned conclusions on the cases in which they are asked to intervene (art. 222 TEC). P. Mengozzi, Instituzioni of Community law and the European Union, Padua, 2003, p. 55: "as regards its functions, the Court of Justice of Justice exercises, first of all, a control of legitimacy on Community acts [when the action is brought by a Community institution or by a Member State; when the when the action is brought by a natural person, the jurisdiction lies with the Court of First Instance.

[84] In this sense, G. Alpa, La normativa sui datos personali: modelli di lettura e problemi esegetici, in Dir. inf. e informatica, 1997, p. 703. Suñé Llinás, The Protection of Personal Data and File Registration. In the collective work Studies on Autonomous Communities and Personal Data Protection. II Meeting between Autonomous Data Protection Agencies Personal, Madrid, 2006, pp. 247-251; Id., Marco Jurídico del Tratamiento de Datos Personales en the European Union and in Spain, in the collective work La armonización legislativa de la Unión Europea, Madrid, 1999, pp. 245-274.

sono garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmato a Roma il 4 novembre 1950, e quali risultano dalle tradizioni costituzionali comuni degli Stati membri, in quanto principi generali di diritto comune[85]".

2.3 Data Protection in the European Union

The EU has indeed put human rights and the principles enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms at the core of its commitments since its establishment.
Against this context, in 1995, with the adoption of Directive 95/46/EC of the European Parliament and of the Council concerning the privacy of individuals with regard to the processing of personal data and the free movement of such data, a significant step was taken in the field of personal data protection[86].
The purpose of this Directive was to standardize the different data protection laws between the Member States, an important necessity for the free flow of data within the EU to ensure security.

Data processed by automated means (such as computer databases) and data in non-automated files are protected by this Guideline (such as paper files)[87]. The Directive does not, however, refer to the processing of data of a strictly domestic or personal nature and of data used for activities outside the reach of EU law, such as protection and public security[88].

[85] See art. 6 T.U.E
[86] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. receive it by October 24, 1998. In Italy it was received with Law no. 675 of December 31, 1996 - Protection of persons and other subjects with regard to the processing of personal data and entered into force in May 1997. Repealed following the coming into force of Legislative Decree 196/2003.Entered into force on December 13, 1995.
[87] Directive 95/46/EC Art. 3
[88] Directive 95/46/EC article 13; Confr. Chapter 5 on PNR

The Directive sets out the uses for which data processing is lawful and positions the individual's consent as a required prerequisite[89] in each case. Furthermore, the transfer of data from a Member State to third countries is allowed only if the recipient has an appropriate[90] level of security.

Article 28 provides for the establishment, at national level, of an autonomous supervisory body for each Member State to supervise data protection: this has led to the establishment of national data protection authorities. On the other hand, the Working Party was formed by Article 29, consisting a representative from each Member State and a representative from the Commission. Its tasks are set out in Article 30 and are mainly the following:

0. *"The Working Party shall[91]":*
    a) *"Examine any question covering the application of the national measures adopted under this Directive to contribute to the uniform application of such measures[92]".*
    b) *"give the Commission an opinion on the level of protection in the Community and in third countries[93]".*
    c) *"advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms[94]".*

[89] Directive 95/46/EC Art. 7
[90] Directive 95/46/EC Article 25; see Chapter 4 on Safe Harbor
[91] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[92] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[93] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[94] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

d) *"give an opinion on codes of conduct drawn up at Community level[95]".*

1. *"If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly[96]".*
2. *"The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community[97]".*
3. *"The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31[98]".*
4. *"The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public[99]".*
5. *"The Working Party shall draw up an annual report and the Council. The report shall be made public persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament[100]".*

Furthermore, if it observes excessive divergence between the laws of the Member States, the Working Group must notify the Commission. It will, on its own initiative, provide advice on matters relating to the security of personal data. Finally, the Annual Report on the general situation concerning the security of the processing of personal data within the Society shall be drawn up.

---

[95] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[96] Ibidem
[97] Ibidem
[98] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[99] Ibidem
[100] Ibidem

In 2001, the Regulation on data security by the Community institutions (Regulation 45/2001/EC) was drawn up in order to expand the protection of personal data to the processing carried out by the Community institutions and bodies, as the implications of the Directive were addressed exclusively to States[101].

In particular, this Regulation creates a supervisory body, the European Data Protection Supervisor (EDPS), which must assess the implementation of data protection laws. If they consider that one of their rights has been infringed by non-compliance with the law, they will obtain complaints from people.

In 2002, a directive to control privacy and electronic communications in more detail was implemented in a more modern way.

The retention of telephone traffic data obtained for surveillance purposes by the police was strictly governed by Directive 2002/58/EC[102].

In addition, in the case of breaches leading to breaches of personal data, providers are obliged to notify the national supervisory authority, and, in certain cases, they must also warn the individuals concerned, depending on the type of data breached.

The adoption of the Charter of Fundamental Rights of the European Union, known as the Charter of Nice, in 2000[103] was another significant achievement of the EU.

---

[101] Law (EC) No 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the security of persons with regard to the collection and free movement of personal data by the institutions and bodies of the Community. In operation as of 1 February 2001

[102] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the collection and protection of personal data in the electronic communications sector (EC) (Directive on privacy and electronic communications). In Italy, the Code on the Security of Personal Data, which entered into force on 1 January 2004, was introduced under Legislative Decree 196/2003.

[103] The European Union's Charter of Fundamental Rights was declared in Nice on 7 December 2000 and in Strasbourg for the second time in December 2007. It also achieves the legally binding power of a treaty with the entry into force of the' Treaty of Lisbon.' The Charter has received a "opt-out" from Great Britain. Poland and the Czech Republic were given an 'opt-out' but have not used it.

In the sense of the defense of the right to privacy and family life, Article 7 states that “everyone is entitled to respect for his private and family life, his or her home and communications”.
The division into two separate articles of the defense of these rights illustrates the development that has occurred in the fifty years since the writing of Article 8 of the ECHR[104].

When the Treaty of Lisbon entered into force on 1 December 2009, the Nice Charter was included as an appendix and thus acquired a legally binding value: pursuant to Article 6 of the Treaty on European Union, the Union 'recognizes the privileges, freedoms and values set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, adopted on December 12, 2007 in Strasbourg.

2.4 GDPR: Structure, Meanings, and Obligations

The new General Data Protection Regulation, also known as GDPR, was introduced through Directive no. 679 of 2016 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, and on the free movement of such data and entered into force on 24 May 2016 but became fully applicable in all Member States as of 25 May 2018.
In essence, the European Parliament, the Council of the European Union and the European Commission aimed to accomplish, through this new legislation, a very specific aim, namely, to reinforce and make more homogeneous, within the Group circuit, the regulations on the security of personal data.

[104] Pizzetti F., Il percorso del Consiglio d'Europa che porta al riconoscimento del diritto alla protection of personal data, LUISS, Available at: http://docenti.luiss.it/privacy-pizzetti/tutelae-protezione-dei-dati-personali-2/sintesi-lezione-6-ottobre-2010/

The GDPR demonstrates the third piece of privacy legislation to be published. Below are the measures that have characterized the legislation on privacy:

- **1996**: Act No. 675/1996, the first Personal Data Protection Act, provides for the obligation to take "minimum" security steps. This was a real revolution, because, for the first time, the concept of 'personal data' was issued, in accordance with the dictates laid down in European Directive 95/46, and its treatment in accordance with the requirements laid down with the requirement to embrace security measures by those who were during their treatment[105].
- **1999**: This was accompanied by Presidential Decree No. 318 of 28 July 1999 specifying the security arrangements. This legislation allowed for the introduction of the principle of processing of personal data but had the drawback of being rambling and much too young[106].
- **2003**: Legislative Decree 196/2003 'Code on the protection of privacy' was issued. Through this measure, the privacy legislation was consolidated into a single text containing an annex (Annex B) which defined security measures. Security steps have been listed. Subsequently, the Code was supplemented by several provisions of the Guarantor's measures which controlled the treatment in the detailed sectors of the market. This was a significant regulation which for numerous market sectors had the merit of shaping privacy[107].
- **2016-2018**: The new Privacy Law, 2016/679 (GDPR) comes into effect on May 25 of this year[108].

Undoubtedly, the GDPR is a novelty that carries with it countless consequences, first of all a complete shift in the approach to data processing that the topic would have.

[105] Amato F., Sbaraglia G., GDPR. Package for survival. Knowing it, implementing it and preventing fines for privacy and data collection, goWare Content Team, 2018.
[106] Amato F., Sbaraglia G., GDPR. Package for survival. Knowing it, implementing it and preventing fines for privacy and data collection, goWare Content Team, 2018.
[107] Ibidem
[108] Ibidem

From a radically different viewpoint from those previously thought, the GDPR (acronym for General Data Protection Regulation) focuses on the value of personal data in our system, qualified as basic human rights by the Regulation itself.
The implications of these predictions are clear and suggest a different approach that the person must take when handling data.

The regulation shall be completely applicable within the European Community as a whole; no particular acts of governments shall be required, except for the adaptation of domestic legislation (on the basis of art. 13 of the European Delegation Law 2016 - 2017). The only purpose of the timeline that elapsed between the date of approval (May 24, 2016) and its entry into force (May 25, 2018) was to allow public and private companies to adapt to this legislation.

It should be remembered that European legislation[109] was intended to enforce continuous monitoring and, thus, the possibility of changing or adjusting the solutions implemented and the frameworks used to ensure that personal data security is as concrete and continuous as possible over the years and consistent with technological advances. This suggests that the GDPR adjustment process that businesses and agencies are expected to undertake did not end but will become a constant fulfillment in the sense of a regularly changing technological and regulatory framework[110].

[109] It is worth noting that, at the time of writing, the Council of Ministers issued the following press release on March 21, 2018: "The Council of Ministers, on the proposal of President Paolo Gentiloni and Minister of Justice Andrea Orlando, approved, in preliminary examination, a legislative decree that, in implementation of art. 13 of the 2016-2017 European delegation law (Law no. 163 of October 25, 2017), introduces provisions for the adaptation of national legislation to the provisions of the European Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data. As of May 25, 2018, the date on which the provisions of European law will take effect, the current Code on the protection of personal data, pursuant to Legislative Decree no. 196 of June 30, 2003, will be repealed and the new regulations on the matter will be represented mainly by the provisions of the aforementioned Regulation that are immediately applicable and those contained in the draft decree aimed at harmonizing the internal system with the new regulatory framework of the European Union in terms of framework of the European Union in terms of privacy protection".
[110] De Stefani F., Practical guide to the new GDPR, Hoepli, Milan, 2018

The very clear purpose of the GDPR, as the Directive itself states, is to harmonize laws on the confidentiality of personal data across Europe by ensuring the security of all EU citizens' data and by providing all organizations with the necessary resources to ensure the confidentiality of such data[111].
In essence, the information referred to in this Regulation relates to personal details defined in the name, address, e-mail address or even photographs relating to the individual. While this Regulation can at first appear as an innovation, it inherits, with a few minor changes, part of the normative structure from Directive 95/46/CE on the security of personal data.

The expansion of the jurisdiction of the Law, which extends to all those organizations that process the personal data of people living within the territory of the European Union, regardless of where that organization is located, is one of the most significant amendments to this new Regulation. This means that the provisions relating to the GDPR extend to the processing of personal data of EU citizens by organizations which do not reside within the territory of the European Union but are capable of providing services and goods to EU residents[112].

Article 1 specifies the purposes pursued by the Regulations and states the following:

(1) *"La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano[113]".*

[111] TOSHIBA – LEADING INNOVATION, GDPR: cosa comporta per la vostra azienda, in Together information, 2016
[112] Implementing a GDPR strategy is critical for all organizations - inaction is not an option, as failure to comply with GDPR requirements can result in penalties of up to EUR 20 million or up to 4 percent of total worldwide annual revenue.
[113] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILof 27 April 2016 on the protection of individuals with regard to the processing of

(2) *"I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche*[114]*".*

(3) *"La direttiva 95/46/CE del Parlamento europeo e del Consiglio ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri*[115]*"*

In essence, in order to ensure the security of the processing of personal data and the free movement of such data, the Regulation puts down specific provisions which ensure the protection of the fundamental rights and freedoms of individuals in this region.

This clause states in the third paragraph that the free flow of personal data must not be limited or prohibited to enforce the privacy of individuals with respect to the processing of personal data[116].

A double purpose of the security of individuals with regard to the processing of personal data and the free flow of data arises from this normative provision: these goals are closely associated with other essential elements defined in the Regulation, namely:

---

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[114] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[115] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[116] DE STEFANI F., The rules of privacy. A practical guide to the new GDPR, Hoepli, Milan, 2018.

1. **Limitation of purpose:** the law stipulates that data controllers and data processors have the right to collect personal data for particular, clear and valid purposes only: this ensures that data must be processed in compliance with a procedure which is completely consistent with those purposes. This means that the processing of the data is limited solely to the reasons for which those data were originally obtained, thus preventing the processing from taking place for another purpose or at a later date[117].
2. **Limitation of storage**: the law specifies that personal data must be stored in a format that requires the data subjects to be known for a time not exceeding the accomplishment of the purposes for which they have been obtained. This implies that businesses are forced to review and validate the data in their possession on a periodic basis, removing data that is no longer appropriate for the purposes for which they were kept[118].
3. **Guarantee of the accuracy and transparency** of the handling of personal data by the data subject in a legal, accurate and clear manner, which allows the data controller to clarify to the data subject the procedure for processing his or her data. This clarification must be clear and easy to understand, and the processing process itself must be carried out in accordance with the data subject's definition[119].
4. **Guarantee of Accuracy**: it is important that regulation is based on the concept of accuracy and guarantees high quality standards in the processing of data: it demands, in effect, not only that data be properly processed, but also that data be regularly checked and updated[120].

[117] "The EU/2016/679 General Data Protection Regulation (GDPR): new rules EU and clarifications on personal data protection" Basic checklist for professional firms, Fondazione Nazionale dei Commercialisti, 2018
[118] "The EU/2016/679 General Data Protection Regulation (GDPR): new rulesEU and clarifications on personal data protection" Basic checklist for professional firms, Fondazione Nazionale dei Commercialisti, 2018

[119] "The EU/2016/679 General Data Protection Regulation (GDPR): new rules EU and clarifications on personal data protection" Basic checklist for professional firms, Fondazione Nazionale dei Commercialisti, 2018
[120] "The EU/2016/679 General Data Protection Regulation (GDPR): new rulesEU and clarifications on personal data protection" Basic checklist for professional firms, Fondazione Nazionale dei Commercialisti, 2018

5. **Guarantee of honesty and confidentiality**: violation of this aspect of the clause. It defines the imposition of heavy monetary penalties on the guilty. In fact, among its objectives, the legislation reiterates the need to process data in such a way as to ensure its security and safety, by means of reasonable technological and organizational steps, to protect it from unauthorized processing, unlawful processing or loss of data. This is one of the most important parts of the provision to which data controllers must pay careful attention, especially nowadays when data protection is at risk in the world of the Internet and its pitfalls. As a result, data controllers are expected to have an effective data protection policy in place that provides them with the tools to disclose any provisions of the provisions found in the regulation[121].
6. **Data minimization:** the regulation establishes that only data that is adequate and relevant: In fact, their processing is restricted only to what is necessary for the pursuit of the purposes for which the data are processed. Unless this is appropriate for legal purposes, data controllers may not collect a large amount of data to ensure future usage or to establish a user profile. The minimization of data follows the goal of restricting objectives, which allows businesses to obtain only the information that is specifically required to accomplish the purposes without going beyond what is necessary[122].

The GDPR consists of 99 articles, split into 11 parts, followed by 173 "recitals." The following is how they are structured:

- "Chapter I: General provisions[123]" (articles 1 - 4).

[121] "The EU/2016/679 General Data Protection Regulation (GDPR): new rulesEU and clarifications on personal data protection" Basic checklist for professional firms, Fondazione Nazionale dei Commercialisti, 2018

[122]"The EU/2016/679 General Data Protection Regulation (GDPR): new rulesEU and clarifications on personal data protection" Basic checklist for professional firms, Fondazione Nazionale dei Commercialisti, 2018

[123] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

- "Chapter II: Principles[124]" (articles 5 - 11).
- "Chapter III: Rights of the interested party[125]" (articles 12 - 23).
- "Chapter IV: Data controller and data processor[126]" (articles 24 - 43).
- "Chapter V: Owner of the processing of personal data to third countries or international organizations[127]" (articles 44 - 50).
- "Chapter VI: Independent supervisory authorities[128]" (articles 51 - 59).
- "Chapter VII: Cooperation and consistency" (articles 60 - 76).
- "Chapter VIII: Remedies, liability and sanctions[129]" (articles 77 - 84).
- "Chapter IX: Provisions relating to specific treatment situations[130]" (articles 85 - 91).
- "Chapter X: Delegated acts and implementing acts[131]" (articles 92 - 93).
- "Chapter XI: Final provisions[132]" (articles 94 - 99).

[124] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[125] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[126] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[127] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[128] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[129] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[130] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[131] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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)

[132] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of

2.5 Court of Justice

The responsibility for ensuring compliance with the laws of the European Union rests with the Court of Justice of the European Union (CJEU). Created in 1952, it has its headquarters in Luxembourg. It gradually saw the extension of its original roles and structure as the European institutions grew. In 1988, the European Union Tribunal was added, and in 2004, the Civil Service Tribunal.
Its aim is to ensure that in every Member State of the Union the rules of the Union are enforced and interpreted in the same manner.

Its activities are:

1. **Interpretation of the law**: a national court can request clarification from the Court as to the interpretation or validity of an EU rule.
2. **Ensuring compliance with the law**: violation proceedings against a national government which are not compliant with EU law can be opened by the European Commission or an EU country.
3. **The annulment of legal acts of the EU**: the national government, the Council of the EU, the Commission, the Parliament, or even private citizens can request the annulment of an act of the EU for legislation which directly affects them.
4. **Sanctions against European institutions:** any person or corporation whose interests are damaged by the Union can bring compensation for damages to the institution before the Court of Justice.

One of the most important decisions of the Court of Justice is the decision regarding the invalidity of the Data Retention Directive with the case "Digital Rights Ireland" of 2014.
By judgment of 8 April 2014, the Court of Justice of the European Union declared the invalidity of Data Retention Directive[133] 2006/24/EC after a

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[133] Directive 2006/24/EC of 15 March 2006 of the European Parliament and of the Council concerning the retention of data produced or processed in connection with the provision of

preliminary reference by both the High Court of Justice of Ireland and the Austrian Verfassungsgerichtshof (Constitutional Court) concerning precisely the validity of that Directive, with specific reference to the fundamental rights to respect private life and the security of personal data, both of which are enshrined in the European Union's Charter of Fundamental Rights.

Specifically, the High Court must settle a conflict between, on the one hand, the company Digital Rights Ireland and, on the other hand, the Ministry of Media, Maritime and Natural Resources, the Ministry of Justice, Equality and Legal Reform, the Commissioner of Garda Síochána (Irish Police Force) and the Attorney General, on the other hand, on the validity of national measures relating to the lawfulness of those measures and to the retention of electronic communications data.

On the other hand, in order to secure the annulment of the national clause transposing the Directive in question into Austrian law, the Austrian Supreme Court has to deal with numerous appeals filed.

The main purpose of the Data Retention Directive is to harmonize the national laws of the Member States relating to the retention of data produced or processed by providers of electronic communications services or of public communications networks which are publicly accessible. The goal will be to ensure that data for the prevention, identification and prosecution of serious crime, in particular organized crime, and terrorism, is available. To this end, the Directive specifies that the suppliers of the services referred to above must maintain the traffic and location data and, in any case, the data required for the identification of the customer, while not allowing the substance of the contact or information consulted to be preserved.

First of all, the Court noted that the data to be maintained enable, in particular, the identity of the person with whom the registered user has interacted and by what means; the time and place of contact to be determined; and the frequency of the user's communication with certain persons over a particular period of time

---

electronic communications services or public communications networks accessible to the public and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

to be known. Such data, taken as a whole, may provide very detailed information on the private lives of the individuals whose data are stored, such as everyday life patterns, places of residence, travels, activities carried out, social relationships and environments visited.

In this regard, the Court found that the Directive unnecessarily interferes with the constitutional rights of respect for privacy and the protection of personal data by requiring the preservation of such data and by allowing the competent national authorities to have access to such data. Furthermore, the fact that data is stored and used without being told in advance by the user may give the data subjects a feeling of constant surveillance. The retention of data for future transfer to the competent national authorities fulfills the goals of public protection in the general interest and the battle against violent crime.

In any case, the Court is of the opinion that the European legislature has exceeded the limits imposed by accordance with the principle of proportionality when implementing the Data Retention Directive: while the retention of data, as set out in the Data Retention Directive, may be considered sufficient for the objective sought by the Directive to be achieved, the extensive and especially extreme interference of the Directive with the fundamental right to privacy has not proven to be adequately restricted to ensure that such interference is effectively limited to what is strictly required.

Currently, this directive:

- It generally concerns:
  I. All individuals
  II. All means of electronic communication.
  III. All traffic data, without differentiation, limitation, or exception[134]
- No objective standards shall be defined by which to ensure that national competent authorities have access to and can use the data for the sole purpose of preventing, detecting, or prosecuting criminal offences. On

[134] Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others

the contrary, it merely refers in a general manner to serious crimes as defined in its domestic legislation by each Member State[135].

- A data retention period of at least six months shall be enforced without any distinction being made between types of data based on their utility with respect to the objective sought. This period is specified as having a minimum duration of six months and a maximum duration of 24 months, but the Directive does not specify the objective requirements by which the retention period should be limited to what is strictly necessary[136].

Finally, the Court found that the Order alluded to the one above:

- Does not have adequate protections to ensure that data is effectively secured against the possibility of misuse and against any unauthorized access to, or misuse of, data[137].
- Enables the degree of protection to be decided by providers based on economic considerations (particularly with regard to the cost of enforcing security measures[138].
- May not ensure that the data is irreversibly lost at the end of their preservation period[139].
- The preservation of data within the territories of the Union is not needed[140].

[135] Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others
[136] Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others
[137] Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others
[138] Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others
[139] Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others
[140] Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others

2.6 Italian Legislative Framework in the matter of Data Protection

Let us start by analyzing what represents the Privacy and Right to Privacy framework at a national level.

The Italian Constitution was born in a period in which the Right to Privacy was not recognized. However, it was possible to find several references between its lines that would later anticipate subsequent regulations.

An example can be found in Art. 14,15 and 21 of the Italian Constitution, respectively concerning the domicile, freedom, and secrecy of correspondence and freedom of expression of thought.

However, the most important reference to Privacy is found in Art. 2 of the Constitution, which includes Privacy in the inviolable rights of man. The constitutional court has also supported with sentence N.38 of 1973[141].

One of the first elaborations regarding the Right to Privacy can be found in the jurisprudence, with a judgment of the Court of Appeal N.4487 of 1956[142], which was based on the appeal of Enrico Caruso[143], with which this right was identified in the protection of strictly personal and family situations and events, which, even if occurring outside the home, do not have a socially appreciable interest for third parties. Such a statement has become fundamental for the balance between confidentiality and the news right, as the dividing line between Privacy and the Right to Information of third parties is now given by the popularity of the subject while specifying that even famous people retain this right, but limited to facts that have nothing to do with the reasons for their popularity.

---

[141] JUDGMENT OF APRIL 5, 1973 Lodged with the Clerk of the Court: April 12, 1973. Publication in Official Journal No. 102 of April 18, 1973.

[142] CASSAZIONE CIVILE - December 22, 1956 no. 4487; Pres. Pasquera P., Est. Avitabile, P. M. Colli (concl. conf.); Associated production company Tirrena Asso film (Lawyer Graziadei) v. Caruso (Lawyer Leone).

[143] Among the most relevant pronouncements are those relating to the Caruso case, sentence no. 4487 of December 22, 1956, sentence no. 990 of April 20, 1963 relating to the Petacci case and, in particular, sentence no. 2129 of May 27, 1975 regarding the case of Soraya Esfandiari.

"Nell'ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto, non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto"[144].

Italy represents one of the last European countries to implement a privacy protection law of general application.
Law 675/1996 on the Protection of Persons and other subjects about the processing of Personal Data implemented by the Directive 95/46/C.E[145]. of the European Parliament and Council on protecting individuals concerning the processing of personal data and the circulation of data.
Art.1 of the law N.675 of December 31, 1996 mentions as follows:

"*La presente legge garantisce che il trattamento dei dati personali si svolga ne l rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle pers one fisiche, con particolare riferimento alla riservatezza e all'identità personal e; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o asso ciazione"*[146].

The decree 196 of 2003 "Code for the Protection of Personal Data," best known as "Testo Unico sulla Privacy" or Privacy Code, came into force on January 1, 2004. This decree has enhanced the legislative path taken by Italy concerning the field of Personal Data, starting from Law 675/96 (as mentioned

---

144 CASSAZIONE CIVILE - December 22, 1956 no. 4487; Pres. Pasquera P., Est. Avitabile, P. M. Colli (concl. conf.); Associated production company Tirrena Asso film (Lawyer Graziadei) v. Caruso (Lawyer Leone).

145 In the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981, the aforementioned Directive 95/46/EC specifies that there is no protection for individuals with regard to the Automatic Processing of Personal Data of 28 January 1981, n.108 of 28 January 1981, ratified in Italy by Law no. 98 of 21 February 1989.

146 Legge n. 675 del 31 dicembre 1996,Tutela delle persone e di altri soggetti rispetto al trattam ento dei dati personali (testo consolidato con il d.lg. 28 dicembre 2001, n. 467) (Pubblicato sulla Gazzetta Ufficiale n. 5 dell'8 gennaio 1997 - Suppl. Ordinario n. 3)

above), specifying and clarifying that Privacy is not only the right for people not to see their data processed without consent, but also the adoption of technical and organizational precautions that everyone, including legal persons, must respect in order to process the data of others correctly.
At a European level[147], this normative is considered the most complete: the legislation is developed in such a way as to devote to the general principles the first part. It gives the necessary definitions for the understanding, among which it is necessary to emphasize those of personal data and the treatment of the latter.

The importance of the rights of the individuals and their value is emphasized by Art. 1 of D.lgs 196/2003. The main objective of this Code is to ensure a high level of protection concerning the processing of data. The most relevant novelty is the one concerning the processing of personal data. It is crucial to bear in mind that among the single text's provisions, the limits within which it is possible to use data, sensitive data, are specified.
Among the many benefits that citizens derive from it, it is essential to point out the rights on:

1. Knowledge of the existence of data concerning the individual
2. Knowledge of the purpose of use of this data
3. The possibility of updating or modifying your data
4. The possibility to delete the processed data

The Italian privacy code[148] is composed of 186 articles divided into three parts, among which there are also attachments. The structure of this Code is explained in the following table:

[147] Already in the seventies, in countries such as Sweden, Denmark, France and Germany, the first 72 regulatory interventions in the field of privacy protection. In the comparative reading of the law n. 675/96 on the treatment of personal data by V. ZENO-ZENCOVICH reads: "In this process of Europeanization of the juridical models Italy has carried out a merely passive role: in the affairs, our Parliament has totally neglected the requirements of adaptation of the legislation of private law of private law legislation, even though they are present and implemented in countries strongly linked to their own systematic and conceptual
conceptual and systematic traditions, such as France and Germany. [...] Italy is therefore, in spite of itself Italy is therefore, in spite of itself, only the "importer" (often with great delay) of Community legislation", 733-734.
[148] The L. 31.12.1996, n. 675 constituted the answer -in some ways convulsive- to a twenty years 73 inertia of the legislator in the sector. Only the pressure of the Community obligation to

PARTS	DENOMINATION	ARTICLES
PART I	General provisions	Art. 1-45
PART II	Provisions relating to specific sectors	Art. 46-140
PART III	Protection of the interested party and sanctions	Art. 141-186

149

Lastly, it is essential to know that the Code on Privacy is also added three attachments: The Code of Ethics, the technical specifications on minimum and security measures, and provisions on non-intermittent processing for judicial and police purposes.

As concerning Privacy and the Internet, the legislation on the protection of personal data does not prevent the acquisition and subsequent processing of data by bodies responsible by law to protect public safety. The law allows the acquisition of such data to prevent, detect, or repress crimes.
Apart from that, the problem of guaranteeing Privacy is pressing on the Internet, where the dissemination of data is easy and fast.
Moreover, this problem is closely linked to the issue of computer security since data theft often occurs through the network. One of the most harmful scourges is spyware, which, often fraudulently installing itself in the victims' personal computers, copies and sends personal data (pages visited, mail accounts, tastes, etc.) to third parties who will then process and resell them for their own

transpose Directive 46/95 and the obvious interest in adhering to the Schengen Convention on the free movement of persons within the European legal space, had finally forced the Parliament to pass that law". V. ZENO-ZENCOVICH, Reasons and objectives of the Code, op. cit., p. 3.
[149] Legislative Decree no. 196 of June 30, 2003 was issued following the delegated law of March 24, 2001, no. 127. Published in the Official Gazette on July 29, 2003 and entered into force on January 1, 2004, it introduced the Consolidated Law on Privacy into Italian law.

economic purposes. In this case, the best defense is to use common sense and appropriate security programs, such as antivirus, firewall, etc.

From a legal point of view, there was, in fact, felt the need to expand the old legal system and, consequently, also the legislation relating to the concept of Privacy which, until not many years ago, dealt exclusively with traditional correspondence and telegraphic and telephone communication.
Today there are various criminally punishable offenses in this field:

1. Unlawful disclosure of personal data.
2. Violation, theft, and suppression of computer correspondence.
3. Disclosure of the content of telematic correspondence.
4. Disclosure of computer or telematic communications.
5. Unauthorized installation of computer interception equipment.
6. Falsification, alteration, and theft of computer communications.
7. Detection of the content of secret computer documents.
8. Unauthorized access to a site.
9. Computer espionage.
10. Computer fraud.

The Unlawful disclosure of personal data on the Internet is a crime provided for by Legislative Decree no. 196 of 2003. When personal (or sensitive or judicial) data is published on the network without the express authorization of the person concerned and outside the cases provided for by law. Classic is the case of a company that publishes its customers' data without authorization and access to the public. The penalty can be up to three years imprisonment.

Indeed, very important was the introduction of the crime of computer fraud, sanctioned by Article 640-ter of the Italian Criminal Code[150], according to which:

[150] See FIANDACA-MUSCO in the same way, Dir. Ink. Pen. P. s., I delitti contro il patrimonio, Bologna, 2002; PAGLIARO, P. s., Delitti contro il patrimonio, Milan, 2003; ANTOLISEI, Manuale di diritto penale, P.s., I, Milan, 2002. See also MASI, Fradi informatiche e attività

"*Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 516 a euro 1032.*

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1549 se ricorre una delle circostanze previste dal n.1 del secondo comma dell'art. 640 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema […]"[151].

As regards the application of the GDPR to the Italian legal system, it should be noted that the text of the Data Protection Code, aligned with the GDPR, was released by the Guarantor Authority on 19 September 2018[152] following the issuance of a decree adapting Italian law to the EU Regulation.

Privacy is a fundamental aspect since various sectors such as condominiums, work and health are governed by it. Therefore, it is critical that the laws required to protect the processing of personal data are followed.

On 19 September 2018, the text of the Italian decree adapting to the GDPR (General Data Protection Regulation) entered into force and replaces the previous Privacy Code with the current rules laid down by the European Union, with the goal of further improving the protection of individuals with regard to the processing of personal data[153]. The aim of the Privacy Code is to reorganize

bancaria, in Rivista penale dell'economia, 1995, which retains that, ex art. 640 ter c.p., the object of crime defense ex. Equality of negotiation is freedom.

[151] Device art. 640 ter Penal Code

[152] GDPR: in the Gazzetta the decree of adaptation LEGISLATIVE DECREE No. 101 of August 10, 2018 Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and which repealing Directive 95/46/EC (General Data Protection Regulation).

[153] GDPR: in the Gazzetta the decree of adaptation LEGISLATIVE DECREE No. 101 of August 10, 2018 Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the

the Personal Data Processing Act by putting together Law 675/1996 and other statutory decrees, regulations and codes of conduct that have followed in recent years in a single framework.

The new European Privacy Regulation introduces important news on the processing of personal data, in particular the rules on consent, information, the right to be forgotten and the limited storage of data have changed.

Several updates to the old Data Protection Code have been brought about by the new European Privacy Regulation (GDPR) which came into force on September 19, 2018.

The main privacy measures introduced were:

- The first reform involves the fundamentals of the legitimacy of the collection of personal data. The GDPR notes that approval must be specific for processing sensitive data. This need not be in written form[154].
- Rules which concern precisely the "communication" and "diffusion" of individuals' personal data. Therefore, for non-compliance with the law, administrative penalties will be enforced[155].
- As regards minors, the new Privacy Regulation establishes that the consent of minors is valid from the age of 16 and that the consent of parents must be given before that age[156].

free movement of such data, and which repealing Directive 95/46/EC (General Data Protection Regulation).

[154] GDPR: in the Gazzetta the decree of adaptation LEGISLATIVE DECREE No. 101 of August 10, 2018 Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and which repealing Directive 95/46/EC (General Data Protection Regulation).

[155] GDPR: in the Gazzetta the decree of adaptation LEGISLATIVE DECREE No. 101 of August 10, 2018 Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and which repealing Directive 95/46/EC (General Data Protection Regulation).

[156] GDPR: in the Gazzetta the decree of adaptation LEGISLATIVE DECREE No. 101 of August 10, 2018 Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and which repealing Directive 95/46/EC (General Data Protection Regulation).

- ❖ The information notice, which must now be clear and simple to understand, is another change introduced by the GDPR. Furthermore, the new regulation states that, in the case of personal data not obtained directly from the data subject, the information must be given within a span which may not exceed 1 month after the data has been collected or at the time of disclosure[157].
- ❖ Furthermore, the amendment provided for in Article 9 Care in the sense of employment relationships, by means of the clause 'Information in the case of receipt of CVs,' specifies that, in the case of receipt of CVs submitted by applicants, employers must supply the information at the time of the first useful communication after the CV has been sent[158].
- ❖ With respect to the right to be forgotten, in situations where the data is processed only on the basis of consent, users can now request the deletion of their personal data if the data is no longer appropriate for the reasons for which it was collected, if the data is processed illegally or if the data subject reasonably objects to its processing[159].

[157] GDPR: in the Gazzetta the decree of adaptation LEGISLATIVE DECREE No. 101 of August 10, 2018 Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and which repealing Directive 95/46/EC (General Data Protection Regulation).

[158] GDPR: in the Gazzetta the decree of adaptation LEGISLATIVE DECREE No. 101 of August 10, 2018 Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and which repealing Directive 95/46/EC (General Data Protection Regulation).

[159] Ibidem

Chapter 3: Main instruments in U.S. legislation regarding Data Protection

3.1. Federal Data Protection Laws: From the Freedom of Information Act (1966) FOIA to the Privacy Act (1974)

At the end of the nineteenth century, the idea of privacy was born in the United States to guarantee the protection of thoughts and feelings, as an extension of the right to private property, against the increasing intrusiveness of printed paper[160]. The content of this right, subsequently established in other countries, has increasingly extended to include the protection of personal data from undue use by third parties. Thus, the right to exercise control over information relating to one's own personal domain has become privacy, allowing one to know at any time whether someone collects information about one's own account and, if so, to determine if such data collection is to be permitted.

However, the protection of privacy in the federal law of the United States of America is very vague and, for the same reason, there is no clear legal definition in the federal system. This is attributable to the fact that many different legal circumstances are included in its notion and, often, very heterogeneous since there are situations varying from the woman's right to end pregnancy, to have access to contraceptives without the risk of state authorities intervening.
Moreover, in addition to the lack of a single federal rule, American privacy legislation is distinguished by the fact that it is governed, so to speak, in a patchwork manner, i.e., in various ways from State to State, in compliance with particular jurisprudential pronouncements, national courts or unique State laws, or by self-regulation by individual agencies or policies of each corporation.

[160] The topic was first addressed, albeit incidentally, in 1888, in a Treaty of Torts by Judge Cooley, in which privacy is defined as the Right to be alone. two years later, the topic was explored further in the essay "The Right to Privacy," 1890, by attorneys Warren and Brandeis.

Without a question, the US law on the security of personal data provides a more fragmented regulatory system. Privacy and personal data are protected at the fundamental level by the Fourth Amendment to the Constitution[161], which provides for any citizen's right not to have his or her person or home invaded by search or seizure unless there is a probable cause that such action may lead to the proof of a crime[162].

Privacy security is not among the rights that are legally guaranteed in the United States of America, but this does not mean that it does not have considerable significance in that system. It definitely does not have the significance that it has in the European framework, where privacy, because it is included in the Charter of Fundamental Rights of the European Union and in the Treaty of Lisbon, is instead configured as a fundamental right of the citizen.

However, the security umbrella provided by the Fourth Amendment suffers from several limitations which severely restrict its scope. First, its protections work only for the benefit of the American population and do not apply to the security of foreign nationals. Moreover, the extent of the defense of the constitutional provision is further limited by the implementation of the so-called 'third-party doctrine' principle, by virtue of which it is not possible for individuals to invoke a reasonable expectation of privacy with regard to information which they themselves willingly transmit to third parties[163]. This means that, if, for example, the telephone service provider has given consent to the use of one's personal data, one cannot argue that such data is then passed to third parties.

In addition, the right to privacy is protected by a sectoral and fragmentary federal statute consisting of a variety of non-harmonized rules, the U.S. The 1974 Privacy Act, which extends only to U.S. citizens and foreigners admitted to the

[161] Atkinson, "The Fourth Amendment's National Security Exception: Its History and Limits, in Vanderbilt L.Rev., 2013, 1343, 1381

[162] The Supreme Court of the United States of America has provided over the years of evolutionary interpretation of the provision in question. While in the case Olmstead v. United States, 277 U.S. 438 of 1928, the applicability of the Fourth Amendment was limited only to physical intrusions, in the case Katz v. United States, 389 U.S. 347, DEL 1967 the scope of application of this provision was extended to telephone interceptions and methods of electronic surveillance, on the basis that it is intended to protect "people not places".

[163] On the "Third Party Doctrine", see Kerr, "The case for the Third-Party Doctrine", in Michigan LR, 2009, 561

status of permanent residents, or the Freedom of Information Act (FOIA), which does not guarantee homogeneous security of the private domain of individuals.

In 1966, the Freedom of Information Act (FOIA) creates the "right to know" in relation to public authorities (federal): it makes all records, files, data collected by the agencies, accessible; (subject to certain assumptions). The Privacy Act was created in 1974, implementing the Freedom of Information Act (FOIA) in two respects[164]:

- Establishes a limit to the circulation of information affecting citizens' privacy[165].
- Encourages the 'right to know' on the part of the person examined[166].

The following components are examined in the definition of the Privacy Act: (1) the requirements for the disclosure of data[167]; (2) the recording of communications[168]; (3) access to records[169]; (4) compliance with agency regulations[170]; (5) agency regulations[171]; (6) civil remedies[172]; (7) guardian rights[173]; (8) criminal penalties[174]; (9) general exemptions[175]; (10) particular exemptions[176]; (11) relationships with other laws[177].

The FOIA was specifically applied to electronic records and archives in 1996 with the enactment by the Congress of the Electronic Freedom of

[164] The legislation on data processing at international level is based on The Privacy Act of 1974" and the "Freedom of Information Act (FOIA)".
[165] The legislation on data processing at international level is based on The Privacy Act of 1974" and the "Freedom of Information Act (FOIA)".
[166] The legislation on data processing at international level is based on The Privacy Act of 1974" and the "Freedom of Information Act (FOIA)".
[167] The legislation on data processing at international level is based on The Privacy Act of 1974" and the "Freedom of Information Act (FOIA)".
[168] Ibidem
[169] Ibidem
[170] Ibidem
[171] Ibidem
[172]Ibidem.
[173] Ibidem
[174] Ibidem
[175] Ibidem
[176] Ibidem
[177] Ibidem

Information Act. This specified the Agency definition (sec. 552f) comprising executive departments; military departments, government agencies, government-controlled bodies, other executive power structures (including the executive office of the Executive Office of the President), independent agencies. Finally, the concept of record has been defined as which means:
Any object, collection, or group of information kept by an agency about a person, including (but not limited to) information relating to: education, financial transactions, medical history, criminal history, and job history, and containing the name or number, mark, or other identifying information assigned to the individual (such as fingerprint fingerprint or voice or a photograph). In reference to documents, the word record and any other phrase used in the FOIA and Privacy Act refers to any information kept by an agency in any format, including electronic format.

As for what concerns the Privacy Act, it was passed by the Federal Congress in 1974, requiring a codification, almost to the letter, of the concepts now defined.
The purpose of the legislative action was precisely to protect American citizens by using increasingly sophisticated computer collection techniques from the increasing number of privacy invasions committed by federal agencies. In addition, after the beginning of '900, *the tort of invasion of privacy*[178] established by the common law of state courts, provided recourse only against invasions of privacy by other private parties or state authorities.
If the breach of privacy came from federal officials[179], it did not, however, provide any solution. For this reason, in an atmosphere of broad political consensus in the US, the Privacy Act saw the light Congress, which was sponsored by the Ford administration[180] as well.

[178] Hong Haeji, "Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao", in Akron Law Review, 2005, Vol. 38 Issue 1, p71-111, 41p.
[179]Frederick Z. Lodge, "Damages under the Privacy Act of 1974: Compensation and deterrence", in Fordham Law Review, March 1984, Vol. 52, p611-636, 26p
[180] Todd Robert Coles, "Does the Privacy Act of 1974 protect your right to privacy? An examination of the routine use exemption", in American University Law Review, Winter 1991, Vol. 40, p957-1002, 46p

This regulatory instrument, which is still in force, applies to *federal agencies*[181] which hold individual-related data contained in a *system of records*.
In particular, it stems from the need to strike a balance between two competing requirements: that of safeguarding the federal government's effectiveness and proper functioning, and that of guaranteeing the right of people to privacy.

To that end, the Privacy Act restricts the ability of federal agencies, though with certain exceptions, to obtain, handle and publish personal information.

To sum up, the guarantee scheme provided by the Privacy Act is based on the following principles:

- The right of the person to monitor the use and distribution of the information included in his or her *record.*
- The right of the person to access, correct or update his or her details.
- Regulation and restriction of personal data collection, storage, use and dissemination.
- Provision of mechanisms for legal action for violations of the Privacy Act provisions.

The first assurance provision means that the disclosure or distribution of an individual's personal data is forbidden by the *federal agency* except on the basis of his or her written request or with his or her consent. However, there are several exceptions to this general ban on the distribution of data without permission, including, in particular, those provided for under the *Freedom of Information Act*. These include, for statistical reasons, the collection or transfer of data for the purposes of public order, public emergency, or for the existence of a judicial mandate. The *routine use*[182] of data by federal agencies offers a further exemption.

The second guarantee clause means the individual's right to have access to his or her own data in order to help him or her to edit, correct or upgrade it.

[181] This includes, but is not limited to, the executive branch, the armed forces, and the federal departments.
[182] United States Department of Justice; The Overview of The Privacy Act 1974

If the Government Agency does not comply with the request for a correction, it is also possible to appeal to the Federal Courts.

The third clause is intended to restrict the power to collect, hold, use, and reveal personal information. Only the information required for the purposes sought by the compilation is permitted to be collected by federal agencies.
Such information should, where possible, be obtained directly from the person and preserved, in any event, in an accurate and complete manner. Federal agencies must also issue a notice in the Federal Register[183] indicating all information systems in their possession and must also keep an accurate statement of all data disclosure and/or distribution activities with an indication of the records in their possession. For their registry officers, federal agencies must also have a code of conduct.

Finally, the fourth provision provides for measures of protection for civil compensation. In particular, under the Privacy Act, in the event that the government agency may not comply with the request to correct or amend the data requested by the affected party, a legal suit for damages can be brought in the first place.

Similarly, civil litigation is also admissible if the federal agency does not authorize the data subject to access his or her own data, or if the data subject is prejudiced by the incomplete or negligent handling of such data.

More broadly, however, the Privacy Act specifies that legal action can be brought in respect of any violation of its provisions, resulting in harm to the person as a direct consequence.

However, there are still several conspicuous holes in the extent of privacy security offered by the Privacy Act[184].

[183] The Federal Register is an official gazette of the United States federal government that is published daily, excluding holidays. It is a source of public knowledge of federal activity, accessible to anyone.
[184] Julianne M. Sullivan, "Will the Privacy Act of 1974 still hold up in 2004? How advancing technology has created a need for a change in the system of record saving", in California Western Law Review 39 no2 395-412 Spr 2003.

First of all, the former stems from its scope of use. The Privacy Act[185], in fact, applies only to the operations of federal agencies. In other words, it is a statute that preserves citizens' privacy only with regard to the operations of agencies of the federal government. They are removed from its application spectrum. And, as noted in the doctrine[186], not all U.S. states have laws to shield their residents from similar invasions of privacy by state entities modeled after the Privacy Act.

Likewise, the Privacy Act only affects the collection of information belonging to U.S. residents or people living in the United States. It does not cover all federal agency data collection or processing operation, but rather the activities of those federal agencies that maintain a record system[187].

Finally, the system of exceptions to the prohibition of disclosure without the consent of the involved party (subject to the number of twelve) constitutes a further restriction on the protection provided by that statute[188].

In breaching these rules, when data is wrongly disseminated, aggrieved parties face significant procedural hurdles before they can seek their recourse in federal court. As well as a two-year statute of limitations from the date of the wrongful exposure to bring the action, they carry the burden of proving damages[189]. In addition, the disclosure of personal information stored in a *system of records* must be prejudicial and the disclosure must be deliberate.

[185] United States Department of Justice; The Overview of The Privacy Act 1974

[186] Amy S. Scarborough , "Nevada needs a Privacy Act: how Nevadans are particularly at risk for identity theft", in Nevada Law Journal, Spring 2007, Vol. 7 Issue 2, p640-663, 24p

[187] Julianne M. Sullivan, "Will the Privacy Act of 1974 still hold up in 2004? How advancing technology has created a need for a change in the system of record saving", in California Western Law Review 39 no2 395-412 Spr 2003.

[188] Julianne M. Sullivan, "Will the Privacy Act of 1974 still hold up in 2004? How advancing technology has created a need for a change in the system of record saving", in California Western Law Review 39 no2 395-412 Spr 2003.

[189] Amy S. Scarborough , "Nevada needs a Privacy Act: how Nevadans are particularly at risk for identity theft", in Nevada Law Journal, Spring 2007, Vol. 7 Issue 2, p640-663, 24p

3.2. Patriot Act 2011: How the "Right to Privacy" Changed after 9.11

The "milestone" of the post-11 September anti-terrorism legislation is the Patriot Act 2001. It constitutes the requisite reading key for a correct understanding of the subsequent law of 2005, which respects its regulatory structure while updating, extending, and deepening some aspects of the original law.

The United States Patriot Act of 2001, an acronym for Uniting and Improving America by Providing Sufficient Instruments Needed to Intercept and Obstruct Terrorism Act of 2001, is the U.S. federal law passed by Congress on October 26, 2001, to counter terrorism by strengthening investigation and control instruments and strengthening security measures. It is easy to imagine how this legislation insists on the realm of personal rights and deeply interferes with the everyday lives of Americans: thus, the increased monitoring of telephone and telematic messages, the use of sophisticated information recognition and storage technology (from medical records to bank data), the collection of fingerprints in libraries, to the possibility of carrying out repeated searches of homes without a warrant. All this under the banner of keeping national security a priority. All this with considerably diminished verification powers by the judiciary. The Patriot Act authorizes the Attorney General to arrest, on the sole basis of rational suspicion of involvement in activities that threaten the national security of the United States, or to dismiss or expel, on suspicion of terrorism, treason, sabotage or sedition, aliens identified as suspected terrorists[190]. All persons classified as' alleged terrorists are also theoretically subject to indefinite detention. The Patriot Act provided that it was only until 31 December 2005 that such extraordinary instruments available to

[190] A reconstruction of the emergency regimes following 2001 taking into account the differences between the systems of constitutional states compared to those characterized by authoritarian regimes can be found in DE VERGOTTINI G., War and constitution: new conflicts and challenges to democracy, Bologna, 2004, 209 ss. For a categorization of the emergent regimes, in diachronic and synchronic key, VEDASCHI A., À la guerre comme à la guerre. La disciplina della guerra nel diritto costituzionale comparato, Turin, 2007, 263-463. On the alternative between formal prediction of states of emergency and their implicit admission there is an old debate on which today see DE MINICO G., Constitution emergency and terrorism, Naples, 2016, 7 ff.

the police and intelligence services could be used, after which a review of the applicable legislative provisions must take place.

The "normalization of the emergency" has recently been accomplished: the contentious provision, signed on March 9, 2006 by President Bush, has relaxed some restrictions, and made 14 of the 16 expiring provisions stable. It is doubtful if the sacrifice imposed by the Patriot Act on the ideals and principles that have made America the emblem of democracy is capable of returning to Americans the serenity required for the pursuit of happiness solemnly proclaimed in the Constitution of 1776 if it is true that September 11 represented a highly destabilizing force for the democratic structure and the conscience of Americans.

The Patriot Act improved drastically the counter- terrorist measures un several significant ways:

- **In order to investigate organized crime and drug trafficking, the Patriot Act requires prosecutors to use existing resources.**
  (1) *Allows law enforcement agencies to use surveillance against various acts of terror*: Before the Patriot Act, courts may authorize law enforcement agencies to perform electronic surveillance to investigate several normal, non-terrorist crimes, such as drug crimes, mail fraud, and passport fraud. Wiretaps to prosecute some, but not all, of the crimes that terrorists frequently commit may also be accessed by police. The law allowed investigators to obtain information while investigating the full spectrum of terrorist-related crimes, including crimes involving chemical weapons, the use of weapons of mass destruction, the killing of Americans abroad and the funding of terrorism[191].
  (2) *Enables federal agents to track advanced terrorists who are trained to evade detection:* For years, "mobile wiretaps" have been used by law enforcement to prosecute ordinary crimes,

[191] The USA PATRIOT Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 26 October 2001

including drug crimes and racketeering. A federal judge may allow a mobile wiretap to target a specific suspect, rather than a specific phone or communication device. Because foreign terrorists are advanced and equipped to thwart surveillance through rapidly changing locations and communication devices such as mobile phones, the law permitted officials to obtain court authorization to use the same methods to monitor terrorists in national security investigations[192].

(3) *Allows law enforcement officials to carry out operations without warning terrorists:* In some cases, if offenders are identified too early for investigation, they can escape, destroy evidence, threaten, or kill witnesses, disrupt contact with associates, or take other steps to avoid arrest. Therefore, under restricted cases, federal courts have long permitted law enforcement to withhold the notification of a judge-approved search warrant has been executed for the subject for a limited period of time. Warning is still issued, but the appropriate delay allows law enforcement time to locate the associates of the suspect, remove imminent risks to our communities, and organize arrests without advance notice of several persons. For decades, these delayed notices search warrants have been used, have proved critical in cases of drugs and organized crime, and have been completely upheld by the courts[193].

(4) *Requires special agents in national security terrorism cases to request an order from a judge to access business records:* Under the Patriot Act, if required to facilitate an investigation, the government can now compel a federal court (the Foreign Intelligence Surveillance Court) to require the creation of the

[192] The USA PATRIOT Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 26 October 2001

[193] The USA PATRIOT Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 26 October 2001

same form of information accessible by grand jury subpoenas. However, this federal court can issue such orders only after the government has shown that the documents in question are necessary for an approved investigation to obtain information about foreign intelligence not relating to a U.S. individual or to protect against international terrorism or covert intelligence activities, given that such an investigation is not being carried out by a U.S. person[194].

- **The Patriot Act has encouraged the exchange and collaboration of knowledge between government agencies so that they can "better connect the dots."**
  (1) The Act eliminated crucial legal hurdles that hindered the communities of law enforcement, intelligence, and national defense from speaking up and organizing their work to protect the citizens of the United States and our national security[195].
- **The law was revised by the Patriot Act to reflect emerging technology and threats.**
  (1) *It helps law enforcement to obtain a search warrant anywhere there has been violence linked to terrorism*: The law specifies that in every district where terrorism-related acts have occurred, warrants can be issued regardless of where they may be executed. This clause does not alter the requirements regulating the availability of a search warrant but simplifies the procedure of the search warrant[196].
  (2) *Allows hacking victims to petition law enforcement for help in monitoring "intruders" on their computers:* This move made technology-neutral in the law; it put cyber criminals on the same

[194] The USA PATRIOT Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 26 October 2001
[195] The USA PATRIOT Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 26 October 2001
[196] Ibidem

footing as physical criminals. Hacking victims can now ask law enforcement for help against hackers, just as burglary victims have been able to invite officers to catch burglars in their homes[197].

- **For those who commit terrorist acts, the Patriot Act strengthened the penalty.**
  (1) *Prohibits terrorist receiving*: A new crime was created by the law that forbids knowingly harboring individuals who have committed or are about to commit a range of terrorist offenses, such as: aircraft destruction; use of nuclear, chemical or biological weapons; use of weapons of mass destruction; bombing of government property; sabotage of nuclear installations; and air piracy[198].
  (2) *Improving inadequate maximum sentences for various crimes that can be committed by terrorists:* Including incendiary attacks, the destruction of power plants, financial support for terrorists and terrorist groups, and the destruction of national defense facilities[199].
  (3) *Increased number of sanctions for treason:* This includes incendiary attacks, killings at federal installations, attacks on communications networks, material support for terrorists, sabotage of nuclear facilities, and interference with flight crew members. Under prior rule, many of the laws on terrorism did not expressly preclude participation in conspiracies to commit the underlying crimes[200].
  (4) Punishes violent attacks on networks of public transportation[201].

[197] Ibidem
[198] The USA PATRIOT Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 26 October 2001
[199] The USA PATRIOT Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 26 October 2001
[200] Ibidem
[201] Ibidem

(5) It punishes bioterrorists[202].

(6) Eliminates the limitations statutes on such terrorist offences and expands them for all terrorist crimes[203].

In order to protect these same people, the Patriot Act takes away much of the privacy rights of a person from the Fourth Amendment. Pre-9/11 legislation set the stage for how law enforcement might necessarily monitor a potential international threat without punishment as an ultimate objective of this sort of intelligence collection under the Patriot Act in domestic cases.

In the United States, the US Patriot Act, passed just a few days after September 11, and the Presidential Military Order issued by George W. Bush in November 2001[204], include the anti-terrorism legislation that most insist on the domain of personal liberty.

For the purposes of this report, the USA Patriot Act[205], enacted by Congress in October 2001, envisages a range of exceptional instruments in order to fight terrorism, including the potential for the Executive to apprehend

[202] Ibidem

[203] Ibidem

[204] Already on September 14, 2001, the Congress approves the Joint Resolution 23 (Authorization for the Use of Military Force, S.J. Resolution 23, 107th Congress, Statue 224, 2001; this Resolution is based on section 5(b) of the War Power Resolution, November 5, 1973, website www.yale.edu/lawweb/avalon/warpower.htm) through which full powers are conferred to the Chief Executive. On September 14, Bush also declares a state of emergency with the Declaration of National Emergency by Reason of certain terrorist Attacks (Proc. 7463, September 14, 2001).

[205] Public Law 107-56, 2001. Here we focus on the effects that the Patriot Act has on the implementation of judicial guarantees and, in particular, on the principle of due process of law. However, the law, composed of ten sections, is wide-ranging and makes many notable changes in the previous legislation, intervening with useful instruments in order to make the fight against terrorism easier and more effective. Among the most important provisions are those aimed at conferring further powers on the investigative bodies which acquire greater freedom of movement in the search for evidence through cable and over-the-air media. The Bank Secrecy Act is amended and money laundering legislation is modified at national and international levels, immigration legislation is modified in order to prevent foreign terrorists from entering the country, action is taken in favor of the victims of terrorism-related crimes, their families and rescuers; new types of crime are created and existing penalties for terrorist crimes are increased, and the intelligence activities of federal agencies, including the CIA, are considerably strengthened. For a thorough examination of the Patriot Act, 2001 see H. Bell, The Patriot Act, Santa Barbara, 2004; A. Etzioni, How Patriotic is the Patriot Act? Freedom vs. Security in an Age of Terrorism, New York, 2004; W. M. Brash, America's Unpatriotic Acts, New York, 2005.

terrorists (or alleged terrorists) judged by military tribunals behind closed doors without the normal assurances of judicial proceedings[206].

President Bush released the Presidential Military Order on the Arrest, Treatment, and Prosecution in the War on Terror[207] of Such Non-Citizens on November 13, 2001, in which he declared "the emergency situation brought about by the terrorist threat requires that, in order to ensure national security, extraordinary measures be taken against non-citizens whom the President believes belong to Al Qaeda or whom he judges to be in some way connected to the terror network".
Accordingly, those identified by the President as suspected terrorists (enemy aliens) will be arrested and detained on the basis of the urgency and the extraordinary nature of the state of emergency[208], in derogation from the procedural protections given by the Constitution.

When we look at the definition of terrorist activity established by the legislation, the first questions arise: this is so vague and indefinite that it allows cases of foreigners engaged in bar fights or domestic conflicts, or those who have provided humanitarian assistance to an agency not recognized by the law, to be included. Aliens categorized as "suspects" are subject to indefinite detention solely and only by virtue of this term, even though they have legal titles, such as asylum, that allow them to live permanently on U.S. soil. The provision of "guilt by association" a legacy of the dark years of McCarthyism, is one of the most troubling aspects of the Patriot Act, on the basis of which the slightest association with a person suspected to be engaged in terrorism, with a "terrorist

[206] R. Dworkin, Terror and the Attack on Civil Liberties, in The New York Review del 6 novembre 2003, 15-17. V. altresì D. Cole, J.X. Dempsey, Terrorismo e Costituzione. Sacrificare le libertà civili in nome della sicurezza nazionale, New York, The New Press, 2002; R.C. Leone e G. Anrig jr., The war on Our Freedom: Civil Liberties in a Age of Terrorism, Washington, The Century Foundation, 2003.
[207] Presidential Military Order: Detention, Treatment and Trial of Certain Non-citizens in the War Against Terrorism, 66 Fed. Reg. 57, 833, 13 novembre 2001.
[208] The Presidential Military Order suggests a strong distinction between citizens with due process rights and non-citizens: non-citizens can be held on military bases and subjected to the authority of military tribunals on the basis of the special powers given to the President of the United States as Commander in Chief.

organization" (among those reported as such by the Secretary of State) or with a "terrorist State" includes a foreigner, immediate deportation[209].

The Patriot Act gives the authorities of Immigration and Border Security the power to seize and detain immigrants for a "reasonable period of time" (it is not stated what "reasonable period of time" specifically means), without charging them and without having to follow any specific procedure. The officials of the Immigration and Naturalization Service (INS) are not required to account for the decision on detention, nor are they required to report to others the personal details and history of aliens detained. This clause also applies to workers at American colleges and universities, as police and campus security officers are deemed to be immigration agents in their own right, in light of the Patriot Act. U.S. institutions with international students are also expected to file detailed reports with immigration authorities on the status and behavior of those students who could request expulsion based on minor offences, such as missing a signature on a form or missing a class without sufficient excuse.

It seems important to remember at this stage that the power of the immigration authorities to detain foreigners has always been limited to the time solely required for the completion of the formalities of expulsion: it is therefore a completely operating prerogative for the power to expel the same subject matter. However, under the terms of the Patriot Act, even people who may not be subject to deportation are now allowed to be kept in confinement by the government. However, under the terms of the Patriot Act, even people who may not be subject to deportation are now allowed to be kept in confinement by the

[209] The federal crime of "guilt by association" had already been reintroduced with the Antiterrorism Act, 1996, enacted by the Clinton Administration after the terrorist attacks on the World Trade Center in 1993 and Oklahoma City in 1995. Because of this offense, people are not punished for the actions they commit, but rather for the fact that they have in some way given support to groups that are disliked by the government. If this rule had been in force in the eighties, anyone who had financed, even minimally, the African National Congress of Nelson Mandela would have committed a crime because the ANC was included in the list of "terrorist groups" drawn up by the State Department. In this regard, see V. D. Cole, J. X. Dempsey, Terrorism and the Constitution, New York, 2002, p.118.

government[210]. The Supreme Court ruled that all criminal charges should be brought against the accused no later than 48 hours after the arrest, with the exception of the "the most extraordinary circumstances[211]". Nevertheless, the use of imprisonment without charges by INS officers is systematic and, by depriving the category of exceptional circumstances of its substance, perfectly aligns itself with the current "normalization of the emergency" pattern, marking an evolutionary direction marked by habit.

Immigration officials have argued that the requirement of "reasonable grounds to believe" in which the Attorney General orders aliens to be detained is essentially the same as the "reasonable suspicion" standard needed to make a detention or search legitimate under the Fourth Amendment[212]. However, if this is the case, the logic does not add up: in fact, if fair suspicion is not even sufficient to authorize an actual criminal law arrest, it is not clear how it would even help to order permanent detention when it comes to the regulation of immigration.

The November 2001 Presidential Order provides that enemy combatants held in detention by the United States (which basically deals with Guantanamo detainees) shall receive "humane and non-discriminatory treatment[213]" and, if brought to trial, be prosecuted by special military courts for breaches of the laws of war and other relevant laws[214].

---

[210] The Supreme Court has ruled, stating that even aliens against whom a deportation order has been issued have a constitutionally guaranteed interest in remaining free, and therefore the INS's authority to keep them incarcerated is limited. V. Zadvydas v. Davis, 121 S. Ct. 2491 (2001)

[211] V. Judgment of the Supreme Court, County of Riverside v. McLaughlin, 500 U.S. 44 (1991).

[212] The Fourth Amendment to the U.S. Federal Constitution provides: "The right of citizens to enjoy security in respect to their person, houses, papers, and things, against unreasonable searches and seizures, shall not be violated; and no judicial warrant shall issue, except upon a well-founded presumption, supported by oath or affirmation of honor, and with specific description of the place to be searched, and of the persons to be arrested, or of the things to be seized."

[213] See also a note dated June 9, 2002, desecreted together with other documents mentioned above on June 22, 2004, in which the Secretary of State, Donald Rumsfeld states that "prisoners captured as part of the war on terrorism are not entitled to the status of prisoners of war under the Geneva Convention (...) but must be treated humanely and, within the limits imposed by military necessity, in a manner consistent with the Geneva Convention of 1949".

[214] Presidential Military Order, cit.

Special military commissions, bodies established ad hoc, sui generis, situated beyond the ordinary paths of justice, both civil and military, are therefore entrusted with the execution of the trials[215]. The President states that the provision of legal proceedings against enemy aliens is only a possibility, with the consequence that those who are not prosecuted, hypothetically, could remain in detention indefinitely or at least until otherwise ordered by the Chief Executive himself[216].This decides the successful implementation, parallel to the administrative one of a judicial procedure, thus avoiding the laws and instruments of assurance and control offered by the legal system. In effect, the United States government has removed the authority of the courts of the country to judge the legitimacy of the acts it has taken against persons alleged to be connected to terrorist groups by entrusting the trials of Guantanamo prisoners to special commissions, to the degree that such sanctions could have led to the violation of the values enshrined in the Constitution[217]and international law norms. However, in order for decisions to be deemed legal, the authority of the military courts should be limited exclusively to determining the breach of the rules of the law of war, while, in specifying the scope of operation of the military commissions. The presidential order of Bush specifies that they are also qualified to judge “other relevant laws” without providing further information as to the existence of those laws. This provision lacks a legal and statutory

[215] V. Presidential Military Order, cit, "adherence to the principles of law and the rules of evidence generally recognizd in federal criminal courts was deemed not practicable "The Presidential Military Order therefore provides for the organization of trials to be held before specially formed military commissions composed of three to seven officers appointed by a special Appointing Authority of the Department of Defense. This Appointing Authority has the power to revoke a member of the Military Commission for just cause and chooses a Presiding Officer for each Commission as well as the Chief Prosecutor and the Chief Defense Counsel from among the judges belonging to the Military Bar. V. Department of Defense Military Commission Instruction No. 3, Responsibilities of the Chief Prosecutor, Prosecutors and Assistant Prosecutors, April 30, 2002.

[216] M.Ratner, Moving Away from the Rule of Law: Military Tribunals, Executive Detentions and Torture, in Cardozo Law Review, vol.24, n.2, April 2003; according to Vice President Dick Cheney "detainees do not deserve the same guarantees and the same means of protection that would be granted to an American citizen who would instead face the ordinary judicial path" V. P.Slevin and G.Lardner, Bush Plan for Terrorism Trials Defended, in Washingthon Post, Nov. 15, 2001, 36, cf. Cheeney

[217] J. Park Taylor, Event Horizon: The Constitution approaches Guantanamo: A legal guide to the U.S. Detainee Cases, in The Montana Lawyer, n.8, 2004, 512-569.

foundation[218].Lastly, both the Geneva Convention and the International Covenant on Civil and Political Rights provide for the inalienable right of any citizen to be tried before 'regularly established' courts, thus removing the authority of ad hoc courts controlled by special rules.

As in regard to Data Protection Law, The Patriot Act grants the right to access personal data kept in the cloud to US law enforcement officials, irrespective of where the data is processed in the world. The Act also includes the right for US law enforcers to prohibit cloud providers from telling their customers that they have had to hand over personal data.in fact, Under the terms of the US Patriot Act, EU-based businesses must report consumer data without the knowledge or consent of the customer to US law enforcers, even though this conflicts with EU data protection laws.

The Patriot Act refers to consumer information kept by any corporation based in:

I. United States.
II. An EU that uses some third party, i.e., a hosting company, to store or process data in the USA.
III. The EU with a parent corporation in the United States.
IV. The EU and the use of data processing facilities by a US subsidiary.

Google in the UK, Amazon in the Netherlands and Microsoft in Germany are all bound by the Patriot Act, to name a few examples. In addition, the BBC, a UK corporation with a presence in the United States, is also bound by the provisions of the Act, along with any EU company that uses software for Blackberry or McAfee virus control.

The provisions of the Patriot Act are in direct contrast with the data security laws of English and the EU. Data privacy laws in the 27 EU countries

[218] Presidential Military Order, cit.; si v. and C. Rosenberg, Detentions at Guantanamo Bay "grave mistake" lawmakers say, in Miami Herald of 7 January 2003, 14.

all forbid the disclosure of personal data without the permission or knowledge of the individual concerned. Such clauses, however, conflict with the responsibilities of the organization to comply with the Patriot Act and to report consumer data secretly to the US authorities. It is difficult to comply with both US law and local data protection regulations applicable to an EU company if an EU company is faced with a Patriot Act disclosure order. The rule of the US will prevail in reality. Well-known multinational tech and search engine firms have admitted that they have revealed EU consumer data as a result of Patriot Act demands.

3.3. Supreme Court Sentences

In terms of its composition, the U.S. Supreme Court is not equivalent to any other court in the world, i.e., judges who are immovable as they can either resign or die. In fact, there is no institutional case equivalent or even comparable to it, neither in the tradition of the so-called legal systems of civil law nor in those of common law.

According to Mason , "the American Supreme Court is the correspondent of the English monarchy. But unlike the Queen who sits on the throne, without real powers it has, instead, real and great power[219]." Therefore, a judicial council, legitimized as a monarchy but with true Republican powers.

The U.S.'s credibility Article 3 of the Federal Constitution of the Supreme Court separates the Supreme Court, on the question of jurisdiction, into that which is competent in matters of dispute between the various States of the Union[220]. Its role is to resolve those conflicts between

[219] Mason, Judicial Activism: Old and New, in 55 Va. Law Review 411 (1969) (Mason , Judicial Activism : Vecchio e Nuovo , nel 55 Va Law Review 411 (1969)

[220] Original jurisdiction: "(a)The Supreme Court shall have original and exclusive jurisdiction of all controversies between two or more States. (b) The Supreme Court shall have original but not exclusive jurisdiction of: (1)All actions or proceedings to which ambassadors, other public ministers, consuls, or vice consuls of foreign states are parties; (2)All controversies between the

the various States of the Union and that corresponds, in our institutional framework, to those conflicts between the Regions and the forces of the State which concern the Constitutional Court in matters relating to the resolution of conflicts, and to those of the judge of appeal.

The Federal Supreme Court exercises this latter form of authority over all lower federal courts[221] and state courts of last resort when a federal matter is involved. These latter functions assigned to the Federal Supreme Court equate, in a broad sense, to the functions attributed to the Italian Court of Cassation by reference to the different courts of appeal by means of an instrument of annulment of judgments. On the other hand, those related to the analysis of the judgments of the Courts of last instance in the theories relating to the issue of federal law are similar to those exercised in relation

United States and a State; (3)All actions or proceedings by a State against the citizens of another State or against aliens". Translation: 28 USC § 1251 - original jurisdiction:"(a) The Supreme Court shall have original and exclusive jurisdiction over all controversies between two or more states. (b) The supreme court shall have original but not exclusive jurisdiction of:(1) All appeals to which ambassadors, other diplomatic representatives, consuls, or vice-consuls of foreign states are parties;(2) All disputes between the United States and a state;(3) All appeals by a State against citizens of another State or against aliens.".

[221] Direct appeals from decisions of three-judge courts: " Ex-cept as otherwise provided by law, any party may appeal to the Supreme Court from an order granting or denying, after notice and hearing, an interlocutory or permanent injunction in any civil action, suit or proceeding required by any Act of Congress to be heard and determined by a district court of three judges". 28 USC § 1257 – "State courts; Traduzione: 28 USC § 1253 - appelli diretti da decisioni dei tribunali tre giudici : " Salvo quanto diversamente previsto dalla legge , ciascuna parte può presentare ricorso alla Corte suprema da una concessione ordine o negare , dopo la comunicazione e l'udito , una pregiudiziale o di ingiunzione permanente in qualsiasi civile azione , causa o procedimento richiesto da qualsiasi legge del Congresso per essere decise da un tribunale distrettuale di tre giudici " . 28 USC § 1257 - "tribunali statali; certiorari. (a)Final judgments or decrees rendered by the highest court of a State in which a decision could be had, may be reviewed by the Supreme Court by writ of certiorari where the va-lidity of a treaty or statute of the United States is drawn in question or where the validity of a statute of any State is drawn in question on the ground of its being repugnant to the Constitution, treaties, or laws of the United States, or where any title, right, privilege, or immunity is specially set up or claimed under the Constitution or the treaties or statutes of, or any commission held or authority exercised under, the United States. (b)For the purposes of this section, the term "highest court of a State" includes the District of Columbia Court of Appeals". (a) Final judgments or decrees rendered by the highest court of a State in which a decision may be due, may be reviewed by the Supreme Court by writ of certiorari in which the validity of a treaty or statute of the United States is drawn in question or where the validity of a law of a State is drawn in question on the ground of its its being contrary to the Constitution, treaties, or laws of the United States, or where any title, right, privilege, or immunity is specially set forth or asserted under the Constitution or treaties or statutes of, or any commission held or authority exercised under, the United States. (b) For purposes of this section , the term " high court of a State " includes the District of Columbia Court of Appeals "

to treaty matters by the European Court of Justice. It should be remembered, however, that its rulings are binding only in the case of the lower federal courts, to be of last resort; conversely, in the case of the state courts of last resort, it rules definitively[222] only on the issue of the federal law posed. In the above cases, the adjudication shall be returned to the State Court if the ruling on federal law has no effect on the section to be determined by the State Court on the matter of State law.

The Federal Supreme Court has the position of protector of the Constitution entrusted to itself by the same Court when the *Marbury vs. Madison*[223] case was decided on the issue of Constitutional validity of Section 13 of the *Judicial Code*[224], i.e., the 1789 Code of Civil Procedure, the notion of "*judicial review"*, the judicial revision of the law capable of declaring it unconstitutional.

The Supreme Court discussed the issue of the prerogatives granted by the constituent fathers to the legislature during the rationale of that decision. He considered that the rights assigned to the legislative authority were objectively restricted, and this on the basis of the fact that, contrary to tradition, the founding fathers specifically wanted a written Constitution to prohibit the legislator from ignoring its prescriptions. Consequently, he found that every regulatory act contrary to the Constitution would always be considered null and void since, unlike the constitutional dictate, that is to say, the nation's fundamental rule. For the Court, therefore, the courts were expected to enforce the Constitution in cases of dispute between the written Constitution and a federal law and ignore the federal law if it was in conflict with the Constitution[225].

[222] Mattei U., Op. cit
[223] Chief Justice John Marshall Marbury v. Madison (1803)
[224] Civil Procedure Code of 1789.
[225] Chief Justice John Marshall Marbury v. Madison (1803)

In the United States of America, regulation of the constitutionality of laws is universal, unlike in Italy, where it can be proposed to the Constitutional Court only by a judge to whom a question of the constitutionality of ordinary law is presented. However, in the American system, since it is considered unconstitutional, the power to disapply a law is not an exclusive prerogative of the Supreme Court, but a responsibility which belongs to all American judges.

Therefore, the Marbury vs. Madison case[226] constitutes a basic jurisprudential arrest in American constitutional jurisprudence and the most contentious element of common law is now the judicial review of state and federal laws.

The most significant privacy decision within this general framework was undoubtedly the *Griswold v. Connecticut*[227] case of 1965, which concerned the issue of the constitutionality of a state law prohibiting the use of contraceptive techniques as a birth control system and the activity of medical assistance in contraceptive practices. The Supreme Court considered that the law of the State of Connecticut prohibiting the use of contraceptives, rather than regulating both the production and sale of contraceptives, was unreasonable. This, in fact, was even older than the Bill of Rights itself in the area of marital relationship privacy.

Accordingly, the legislation was not, in the Court's opinion, compatible with the principle that the State's regulation and prevention purposes should never restrict or nullify fundamental freedoms which are constitutionally covered and instead ruled unconstitutional[228] by way of

[226] Chief Justice John Marshall Marbury v. Madison (1803)

[227] GRISWOLD ET AL. v. CONNECTICUT No. 496 SUPREME COURT OF THE UNITED STATES 381 U.S. 479; 85 S. Ct. 1678; 14 L. Ed. 2d 510; 1965 U.S. LEXIS 2282 March 29, 1965, Argued June 7, 1965, Decided.

[228] Griswold vs. Connecticut, cit. sub note 30 ""(...) would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship(...)." Translation: Griswold v. Connecticut, cit. . sub note 30 " " (...) will it allow police to search the sacred

the fact that they did not guarantee the right of married couples to have recourse to contraceptives.

The Supreme Court affirmed with the decision that in the U.S. There was an implied right to privacy in the Constitution, known as *the Penumbra Principle*[229].

In the end, it was stated in the *Griswold vs. Connecticut decision* that each of the provisions of the Bill of Rights covered various aspects of privacy.

The Supreme Court applied the principle of penumbra to the Equal Protection Clause in *Eisenstadt vs. Baird*[230], i.e., the equal protection of the Fourteenth Amendment clause, expanded the right to use contraception to unmarried persons, on the basis that privacy is to be interpreted as the individual's particular right because of that.

However, in *Loving vs. Virginia*[231], the Supreme Court ruled the statute banning mixed marriages in conflict with the Fourteenth Amendment unconstitutional, arguing that the right to marry is a personal interest protected by the Constitution.

Subsequently, the Court partly modified its orientation in the *Roe vs. Wade*[232] case of 1973, further clarifying the definition of the "*privacy*

precincts of marital bedrooms for telltale signs of contraceptive use ? The idea is repugnant to notions of privacy surrounding the marriage relationship (...)

[229] GRISWOLD ET AL. v. CONNECTICUT No. 496 SUPREME COURT OF THE UNITED STATES 381 U.S. 479; 85 S. Ct. 1678; 14 L. Ed. 2d 510; 1965 U.S. LEXIS 2282 March 29, 1965, Argued June 7, 1965, Decided.

[230] EISENSTADT, SHERIFF v. BAIRD No. 70-17 SUPREME COURT OF THE UNITED STATES 405 U.S. 438; 92 S. Ct. 1029; 31 L. Ed. 2d 349; 1972 U.S. LEXIS 145 November 17-18, 1971, Argued March 22, 1972, Decided.

[231] Loving v. Virginia (No. 395), WARREN, C.J., Opinion of the Court SUPREME COURT OF THE UNITED STATES 388 U.S. 1 Loving v. Virginia APPEAL FROM THE SUPREME COURT OF APPEALS OF VIRGINIA, No. 395 Argued: April 10, 1967 --- Decided: June 12, 1967

[232] This case was brought to light by a pregnant woman. It concerned the supposed unconstitutionality at any point of pregnancy of a Texas law banning abortion, except when it was necessary to save the mother's life.

zone" already stated in the *Griswold vs Connecticut*[233]. In this ruling, the Court held that the right to terminate a pregnancy by abortion was a right protected by the right to privacy in the Constitution. In that decision, the Court held that a right covered by the constitutional right to privacy was the right to end a pregnancy by abortion.

However, that right was not absolute because it had to be balanced with the other essential interests of the State and that its restriction by statute could be justified only in the light of the pre-eminent interest of the State, which was not recognizable in the case at issue and therefore ruled Virginia's law unconstitutional.

In the *Roe* Judgment, the Court ruled that the right to privacy was based on the Fourteenth Amendment, contrary to what had been stated in the *Griswold* Judgment. The *principle of penumbra* was therefore set aside because the Court claimed in the last sentence that only the fundamental rights of the individual, or those which are implied in the notion of individual liberty, are secured by privacy. From the jurisprudence of the Supreme Court studied, it would seem almost likely to deduce that privacy, far from configuring the individual's autonomous right, is instrumental only in the defense of the fundamental rights established by the Court itself.

There have been several efforts to extend the protection of privacy since *Roe* to illustrate this, but with occasional exceptions, such as the invalidation of legislation banning the selling of contraception to minors, the Court has often declined to widen the scope of Roe's jurisprudence.

In this respect, the Court initially considered that the right to engage in same-sex relationships was not appropriate to extend privacy

[233] GRISWOLD ET AL. v. CONNECTICUT No. 496 SUPREME COURT OF THE UNITED STATES 381 U.S. 479; 85 S. Ct. 1678; 14 L. Ed. 2d 510; 1965 U.S. LEXIS 2282 March 29, 1965, Argued June 7, 1965, Decided.

protection, but then partially corrected its course by extending protection to individual sexual activities in general.

In *Lawrence v. Texas*[234], by declaring unconstitutional a Texas law that qualified homosexual relations between consenting adults as a crime, the Court overturned *Hardwick jurisprudence*.

Finally, the Court also denied the extension of the constitutional right to privacy to the government's collection of personal data in the case of *Whalen vs. Roe*[235]. In the case of *Katz vs. United States*[236], the Court stated that the final guarantors of *individual privacy* are the States and not the Federal Government.

For these reasons, several states, such as Florida, California, Alaska, and Montana, updated their state constitutions to include specific privacy clauses during the period between 1968 and 1980.

3.4. The Californian Framework in the matter of Data Protection

The Californian framework in matter of data protection tends to follow policy tendencies similar to what can be seen in the European Union.

Article 1 of Section 1 of the California Constitution establishes an inalienable right for persons to seek and gain privacy. It is possible to enforce this right to privacy against private individuals[237].

---

[234] SUPREME COURT OF THE UNITED STATES Syllabus LAWRENCE ET AL. v. TEXAS CERTIORARI TO THE COURT OF APPEALS OF TEXAS, FOURTEENTH DISTRICT No. 02–102. Argued March 26, 2003—Decided June 26, 2003

[235] WHALEN, COMMISSIONER OF HEALTH OF NEW YORK v. ROE BT AL. APPEAL FROM THE -UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK No. 75-89. Argued October 13, 1976-Decided February 22, 1977

[236] KATZ v. UNITED STATES, 389 U.S. 347 (1967) 389 U.S. 347 KATZ v. UNITED STATES. CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT. No. 35. Argued October 17, 1967. Decided December 18, 1967.

[237] See Hill v. Nat'l Collegiate Athletic Ass'n, 26 Cal. Rptr. 2d 834, 842 (Cal. 1994).

A person may bring a claim in court to enforce this constitutional right, where he or she must prove that:

- In the specified case, they had a fair privacy expectation.
- One that society acknowledges is the desire in privacy.
- The invasion of the privacy of the complainant is a "egregious breach of social norms[238]."

Under Section 4 of Division 3 of the California Civil Code and the California Consumer Privacy Act Rules, the California Consumer Privacy Act[239] of 2018 provides the most detailed general legislative structure for data privacy in the United States.

The CCPA came into effect on 1 January 2020 and became enforceable on 1 July 2020 by the Attorney General of California. On 14 August 2020, the CCPA Regulations came into effect and have the same force of law as the CCPA.

For protected organizations that collect “personal information” about “consumers” and offer new rights to such persons with regard to their personal information collected by those organizations, the CCPA imposes new responsibilities. Consumers are described as natural people who are residents of California:

- Living in California at present (more than temporary)
- For a temporary reason, outside the state, as per Section 17014 of Title 18 of the California Code of Regulations

The Act applies to subsidiaries, associations or other legal entities which share a trademark, which collect personal information from consumers or on whose behalf such information is collected and which decide the purposes and means of the collection of personal information relating to consumers and which, in the State of California, have economic interests which meet the following thresholds:

[238] See Hill v. Nat'l Collegiate Athletic Ass'n, 26 Cal. Rptr. 2d 834, 842 (Cal. 1994).

[239] The CCPA Regulations were first published in draft form on 10 October 2019 and underwent several formal comment periods and modified drafts. The final version of the CCPA Regulations were approved by the Office of Administrative Law on August 14, 2020 and went into effect immediately.

- Gross annual sales in excess of $25 million.
- transactions on an annual basis, on their own or with other third parties, acquiring, selling, or disclosing, for commercial purposes, on their own or with other third parties, personal details of 50,000 or more customers, households, or equipment.
- At least 50 percent or more of the annual sales stems from the selling of personal information to customers[240].

Therefore, if the companies referred to above are "selling" or "disclosing" customer (or even household or device-related, internet-related, or IoT-related) personal information[241] as citizens of the State of California, they are subject to such obligations.

Such obligations concern businesses falling within the scope of the CCPA are expected, first and foremost, to maintain, on their website, a privacy policy updated at least annually, including a summary of user rights and the nature and type of personal information and a list of information sold or disclosed in the preceding year.

The following privileges are given to consumers:

- *Right to opt-out:* customers may request that businesses and/or their partners not reveal or sell their personal details. In this case, after exercising the right to opt-out, the company must refrain from offering to collect the consumer's information again for at least 12 months[242].

[240] California Legislative information, AB-375 Privacy: personal information: businesses. (2017-2018) (2018-2019)

[241] Included in the category of personal information: information that identifies, directly or indirectly or is directly or indirectly linked to a consumer or household, such as (i) identifying information, (ii) commercial information, (iii) biometric data (iv) internet connection or online browsing information (e.g., history, information from app and device interconnections), (v) geolocation data, (vi) auditory, visual, olfactory, electronic, thermal, or similar information (vii) professional information (viii) academic information (ix) information that enables consumer profiling. Excluded from the scope are public information and information in aggregate or de-identified form- AB 375, Sec. 1798.140., sub-section (o)

[242] Included in the category of personal information: information that identifies, directly or indirectly or is directly or indirectly linked to a consumer or household, such as (i) identifying information, (ii) commercial information, (iii) biometric data (iv) internet connection or online browsing information (e.g., history, information from app and device interconnections), (v) geolocation data, (vi) auditory, visual, olfactory, electronic, thermal, or similar information (vii)

- *Right of access*: the user may request whether or not there is a sale or disclosure of personal information relating to him or her, often involving third parties, and which information is the subject of the sale or disclosure, for a period of 12 months prior to the request[243].
- *Right of erasure*: the customer can request data collected by the company and its suppliers to be erased[244].
- *Right not to be discriminated against* customers who have exercised their right of withdrawal must not be discriminated against (e.g., by unequal treatment of costs, incentives not to withdraw, or by giving greater benefits to those who have not exercised their right)[245].
- *Right to Feedback*: Within 45 days of their submission, the user must receive feedback. However, upon reason, the company can extend its response from 45 to 90 days[246].
- *Right to action:* If a person wishes to bring legal action (right to action) against a corporation, he or she can do so only: (a) by providing notice to the company for at least 30 days, and (b) by involving the Attorney General of California[247].

professional information (viii) academic information (ix) information that enables consumer profiling. Excluded from the scope are public information and information in aggregate or de-identified form- AB 375, Sec. 1798.140., sub-section (o)

[243] Included in the category of personal information: information that identifies, directly or indirectly or is directly or indirectly linked to a consumer or household, such as (i) identifying information, (ii) commercial information, (iii) biometric data (iv) internet connection or online browsing information (e.g., history, information from app and device interconnections), (v) geolocation data, (vi) auditory, visual, olfactory, electronic, thermal, or similar information (vii) professional information (viii) academic information (ix) information that enables consumer profiling. Excluded from the scope are public information and information in aggregate or de-identified form- AB 375, Sec. 1798.140., sub-section (o)

[244] Ibidem

[245] Ibidem

[246] Ibidem

[247] Included in the category of personal information: information that identifies, directly or indirectly or is directly or indirectly linked to a consumer or household, such as (i) identifying information, (ii) commercial information, (iii) biometric data (iv) internet connection or online browsing information (e.g., history, information from app and device interconnections), (v) geolocation data, (vi) auditory, visual, olfactory, electronic, thermal, or similar information (vii) professional information (viii) academic information (ix) information that enables consumer profiling. Excluded from the scope are public information and information in aggregate or de-identified form- AB 375, Sec. 1798.140., sub-section (o)

On November 3, 2020, by a vote of California voters, the proposed extension of the CCPA, by the text of the California Privacy Rights Act 2020, was approved and is intended not to repeal, but to complement the provisions of the CCPA. It will enter into force on 1 January 2023.

Some of the latest features the CPRA has implemented include:

- Right of rectification: the customer shall have the right to order companies to rectify their inaccurate personal information up to that point.
- Sensitive data: A new type of data is added by the CCPRA, i.e. sensitive data, such as: social security number, driver's license number, passport number, financial account information, credit or debit card information, precise geolocation information, racial or ethnic origin information, religious or political beliefs, trade union membership, consumer sexual orientation or life, and health, information contained in consumer mail, e-mails, and messages, except if intended for business.
- Right to "Limit Use of my Sensible Personal Information": Privacy policies should include a section allowing users to access the request directly in order to restrict the use of their confidential information[248].
- The new Privacy Regulator: an agency (state or federal) will be formed to replace the Attorney General of California (until now the only authority to deal with any consumer acts or complaints) and will have the sole purpose of providing for consumer data security regulations[249].
- Increased responsibility for data breach: users would be able to take private action to compromise email addresses, in accordance with login or security questions and answers that may provide access to the account of a customer[250].

[248] "California Approves the CPRA, a Major Shift in U.S. Privacy Regulation", National Law Review, Volume X, Number 322
[249] "California Approves the CPRA, a Major Shift in U.S. Privacy Regulation", National Law Review, Volume X, Number 322
[250] "California Approves the CPRA, a Major Shift in U.S. Privacy Regulation", National Law Review, Volume X, Number 322

- ❖ Minimization of data and overall retention period: For each type of data it collects, the organization would have to notify its customers about the retention period. The customer is entitled to request the use of only the information required for the purposes defined by the business[251].
- ❖ Introduction of "sharing" data: unlike sales, the definition of data sharing will be explained and controlled, and the current concept of "disclosure" will also be introduced[252].

Of course, the California Privacy Act review should not be differentiated from a direct contrast with the GDPR. In particular, the current CPRA seeks to complement the previous version of consumer data protection legislation with requirements which the European Regulation seems to have provided for.

It is important enucleate, however, several points of distinction:

- ❖ *Scope*: The law is intended solely for the safety of citizens of the State of California and is intended for particular businesses, defined on the basis of requirements relating to the size and form of company of an entrepreneur.
- ❖ *Legal basis*: The law presupposes that corporations can use the personal information of customers but does not discuss the manner and basis on which such information is collected.
- ❖ *Measures:* While there are frequent references to duties and responsibilities, there are (yet) no clear indications as to how to use customer data.
- ❖ *Roles:* the roles played by corporations are paid little attention. Third parties, beneficiaries of the selling, exchange or disclosure of personal information shall be referred to, but they shall not be controlled by the attribution of responsibilities[253]. Likewise, there is no person who is internally responsible for checking that undertakings comply with the

[251] Ibidem
[252] Ibidem
[253] Sec. 5, THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020, "Amendments to version 3"

provisions relating to the security of personal information of consumers, such as the European DPO.

- *Transfers:* There is a lack of specific regulation on the transfer of personal information, in particular in view of the fact that many companies based outside the State of California or the United States may actually have business interests in California and target California consumers, not to mention third-party suppliers or contractors who are associated with the regulation and may be located in third-party suppliers or contractors.

It can also be seen that while the CCPA and CPRA regulate the "core" of the use of data, concentrating on disclosure, selling, and sharing as well as user rights already in place, the GDPR provides guidelines for legal entities that process it, from design to eventual preservation of personal data.

Chapter 4: The transfer of Personal Data to third countries

4.1. An introduction to the EU regime for the transfer of Personal Data to third countries

A very high European standard of personal data security has been established by Directive 95/46/EC, which entered into force on 25 October 1998. Chapter IV of the Directive deals with the transfer to third countries of personal data (not belonging to the EU or the European Economic Area: Norway, Iceland, Liechtenstein) and, in compliance with Article 25(1), with:
"Member States shall provide that the transfer to a third country of personal data that are being processed or intended to be processed after the transfer may take place only if the third country in question ensures an adequate level of protection, without prejudice to national measures implementing other provisions of this Directive[254]*."*

The Commission, which may make rulings, has the authority to assess whether a country offers an appropriate standard of security.
Decisions on adequacy, with the constructive view of the Working Group on Article 29. Article 25, paragraph 2, states that:
"*The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer or a category of data transfers; in particular, the nature of the data, the purpose of the proposed processing operation, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third country in question, and the professional rules and security measures in force*

[254] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal No L 281 of 23/11/1995 p. 0031 – 0050.

there, shall be taken into consideration. country in question, as well as the professional rules and security measures observed there[255]."

It is also necessary to remember that, for the purpose of determining the degree of protection, what needs to be evaluated by the Commission is not only the legislation in effect in the country concerned, but also all non-binding regulations and safety standards. Self-regulation, i.e., the rules of actions followed by companies or whole sectors, is also important to remember.
In this regard, the working group assumes that it is not so much the size of the organization that should be evaluated when reviewing this instrument, but rather the successful observance of the rules and the capacity to enforce penalties.
Furthermore, if self-regulation includes the whole market, this constitutes a benefit in terms of clarity, as opposed to a fragmented system that can be frustrating for the customer.
The probability of data transfer to companies which do not share the same regulatory codes is another factor that should be carefully considered. Rather, it should be forbidden to pass data to those who do not provide sufficient protections.

It is also very important for the assessment to ensure that the guidelines are straightforward, that they are written simply and without any potential ambiguity, and that they can even include examples.
Finally, according to the Working Group, three characteristics of self-regulation should be analyzed in order to identify them as necessary.
Respect for the rules is the first. The presence of a penalty scheme in this regard will provide a fair assurance for the security provided by the Code.

[255] JUDGMENT OF THE COURT (Grand Chamber),6 October 2015 (*), 'Reference for a preliminary ruling - Personal data - Protection of natural persons with regard to the processing of such data - Charter of Fundamental Rights of the European Union - Articles 7, 8 and 47 - Directive 95/46/EC - Articles 25 and 28 - Transfer of personal data to third countries - Decision 2000/520/EC - Transfer of personal data to the United States - Inadequate level of protection - Validity - Complaint by a natural person whose data have been transferred from the European Union to the United States - Powers of the national supervisory authorities", In Case C-362/14.

The second is the existence of an independent body which monitors and offers assistance in accessing data retention.

When the rules are broken, the last function that should be present is remedial mechanisms. Compensation for losses sustained should be included.

Subsequently, Article 26 of the Directive lays down the cases in which a transition to a country guaranteeing adequate security is needed.

By way of derogation, however, from Article 25 (2). These circumstances indicate that:

a) "The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards."[256]
b) "The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.[257]"
c) "The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.[258]"
d) "The transfer is necessary for important reasons of public interest.[259]"
e) "The transfer is necessary for the establishment, exercise or defense of legal claims.[260]"
f) "The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent[261]."
g) "The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and

[256] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted on 25 May 2018
[257] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted on 25 May 2018
[258] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted on 25 May 2018
[259] Ibidem
[260] Ibidem
[261] Ibidem

which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case[262]".

Paragraph 2 of Article 26 of the Directive also provided for a further hypothesis, given at the request of the controller by the authorization of the State of the European Union, of care properly recorded by "adequate" contractual level guarantees for the security of the personal data of the individual concerned who is the subject of the transfer[263]. This discipline was later transposed into different national legislation, which could easily allow for exceptions in the absence of strict European Union criteria. In Italy, the Privacy Code under Title VIII has controlled the matter for years[264].

Needless to say, the development and evolution of disciplines did little but significantly diversify them, at least until the issuance of Regulation (EU) 2016/679[265], which dictated its final stabilization in the European Union and, in accordance with Council of Europe Convention 108/1981[266], constituted the only internationally binding instrument for the subject matter.

In Chapter V of the GDPR, Articles 44 to 50, the administrative placement of the subject matter relating to the transfer of personal data to third countries or foreign organizations is laid down. Article 44 is the "manifesto" of the limitations imposed by the Law with respect to the privacy of personal data. Unlike Directive 46/95/EC, there is no concept of "transfer" in the GPDR.

---

[262] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted on 25 May 2018

[263] V. Colarocco, The transfer of data to third countries, in the process of the GDPR, edited by G. Cassano, V. Colarocco, G. B. Gallus, F. P. Micozzi, 236.

[264] Code for the protection of personal data, d. lgs. 196/2003, available here: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.5.

[265] General Data Protection Regulation (GDPR), available here: https://www.garanteprivacy.it/documents.

[266]The Italian text of the Convention is available here: https://rm.coe.int/CoERMPublicCommonSearchServices.

In any case, it must be considered that it occurs if the physical transfer of personal data beyond the *European Economic Area*[267] takes place. Furthermore, the doctrine seems to accept that the mere movement of personal data through instruments which are not physically present in the territory of the Union does not constitute a hypothesis of transfer, even in the light of the literal date of Article 44 of the GDPR.
As already provided for in the previous European and national contexts, Article 45 subsequently allows for the legality of the transition to be subject to an adequacy decision adopted by the Commission.

To date, for only 11 countries: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, the Bailiwick of Jersey, New Zealand, Switzerland and Uruguay, the Commission has recognized an adequate level of protection[268]. Argentina, Canada and Switzerland, whose federal laws have been considered relevant, are perhaps the most important examples.
According to the requirements of the society and in which appropriate communication on privacy security has been found. On July 26, 2000, Switzerland was the first country to obtain a positive verdict on adequacy[269].
The Swiss Federal Act on Data Protection (SFADP) was considered in the decision and some reservations about it were raised by the working group[270].

The weaknesses highlighted by the Working Group's review relate to the transfer to non-restricted third countries, to the absence of an obligation to notify interested parties about the processing of the data, to the absence of instruments to settle disputes. However, thanks to the inclusion of some clauses to better

[267] See again G. M. Riccio, GDPR and privacy regulations, 396, cit.
[268] Commission decision on the level of adequacy of the protection of personal data of third countries third countries, Available at: http://ec.europa.eu/justice/dataprotection/international-transfers/adequacy/index_en.htm
[269] 2000/518/EC: Commission Decision of 26 July 2000 on the adequacy of the protection of personal data in Switzerland pursuant to Directive 95/46/EC.
protection of personal data in Switzerland under Directive 95/46/EC, Available at:
http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32000D0518&from=EN
[270] Opinion No 5/99 on The level of protection of personal data in Switzerland: http://ec.europa.eu/justice/data-protection/article29/documentation/opinion recommendation/files/1999/wp22_en.pdf

protect personal data in the Constitutions of most cantons, the Commission has decided to take a positive view of the progress made to align with European standards.

As is not exhaustively summarized, the new framework developed by the European Regulator on the cross-border transfer of personal data seems to take up previous disciplines, but with the requisite clarifications in terms of the development of the underlying technologies, allowing a versatile and at the same time robustly secured approach to the possibilities of "international" flow of personal data guaranteed by effective and rapid protection[271].

The issue of the effectiveness of these rules is what continues, today as then, to trigger anxiety for the interpreter. The vagueness of the language of the exceptions to the move prohibition provided for in the second paragraph of Art. 49, par. 1, the contractual clauses usually used in business practices which often remain a 'dead letter,' the material inability for the supervisory authorities to systematically check compliance with the Regulation, remains an important problem which must be resolved as soon as possible.

Increasingly, there is a need to prevent personal data from being 'profiling goods' sold to the highest bidder abroad, without any confidentiality security scruples and without any obstacles to preventing access to one's own information, which, after all, can be accessed for the most varied and, in many cases, not exactly legal purposes.

4.2. Safe Harbor Agreement and the Case Schrems I

There are no frontiers for the transfer of personal data. Within fractions of a second, the internet offers the possibility to send, copy, and process vast data sets. Thus, various systems of law and different criteria collide. The processing of personal data is handled seriously by Germany and the European Union. The principle holds, therefore, that personal data should only be obtained,

[271] The duty to include transfers of personal data abroad or to foreign organizations in the Registry pursuant to Article 30 of the GDPR is also of interest.

processed, and used in compliance with a legally defined structure. The processing of such data is, however, limited to its purpose and necessity. This involves a comprehensive balancing of the needs of the citizens and authorities concerned, as a general rule.

This interpretation stems from the German Federal Census Act
In 1983, the Constitutional Court laid down guidelines for the governmental treatment of citizens' personal data[272]. The harmonization of European data security standards has emerged as a result of the ongoing implementation of this general law. This began with the development of the European Data Protection Directive in 1995 and continues with the General Data Protection Regulation of the European Union, which allows for a thorough harmonization of data protection legislation. The United States of America has a more generous view of data security, in comparison to that[273]. There is currently no clear definition of data security for personal data. On the other hand, there are only area-specific regulations without a central data protection authority[274]. In order to deal with personal data, only a few federal states have legal requirements. Moreover, most of the US-American data security laws are not, or are only limited to, available to EU residents[275].

The gaps between the legal areas require that only a promise of a high degree of privacy[276] allows the export of personal data from the European area to be considered allowable.

Ultimately, the major data processing firms, such as Facebook, Google, and Amazon, have their headquarters in the United States of America. It must also be borne in mind, apart from secure basic requirements for private companies, that public agencies in the US have far-reaching competences with

[272] BVerfG, NJW 1984, p 419.
[273] 4 Börding, CR (2016), p 434
[274] Ibidem
[275] Böhm, A comparison between US and EU Data Protection Legislation for Law Enforcement, 2015, p 69 et seqq.
[276] Considering the legal procedure see EuGH, Decision of 6 Oct 2015, C-362/14, MMR 2015, p 753 et seqq. with notes from Bergt

regard to the disclosure of personal data stored and processed and that they make extensive use of it[277].

While in 2015 the former "USA Patriot Act" was replaced by the "USA Freedom Act" and the intelligence services are now subject to tougher formal criteria, it remains to be seen which realistic approach and which advances in data security will allow their entrance into the United States[278]. It is therefore necessary for the European Union to develop secure and clear data transfer regulations between Europe and the US. This provides the legal basis for the EU Data Protection Directive, the Federal Data Protection Act and the Single State Data Protection Acts.

With the advent of emerging technology and the Internet in the 1990s, the so-called Safe Harbor Agreement implemented regulations governing the transfer of personal data between Europe and the US. Non-governmental organizations (NGOs) and national and EU institutions expressed their concern, arguing that the protection of personal data of EU citizens was not adequate. The CJEU eventually ruled on the issue, making it necessary to introduce a new regime.

Directive 95/46/EC, adopted by the Parliament and the Council on 24 October 1995[279], on the security of individuals with regard to the processing of personal data and on the free movement of such data, states that a transfer of personal data to a third country may take place only if the third country concerned guarantees a "adequate level of protection" (Art. 25, para. 1).

The Commission must determine the adequacy of the security. Where an appropriate degree of security is not guaranteed by the State, the transfer remains

[277] See Electronic Frontier Foundation 2015, Who Has Your Back? https://www.eff.org/who-hasyour-back-government-data-requests-2015.

[278] Byers 2015, USA Freedom Act vs. USA Patriot Act, http://www.politico.com/story/2015/05/usafreedom-act-vs-usa-patriot-act-118469

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

possible by way of derogation from Article 25. The conditions of such derogations are stated in Art. 26[280].

Yet, if data transmission were only possible on the basis of derogations signed by private operators, it would be counterproductive to EU-US ties. It is precisely for this purpose that the EU and the US introduced "Safe Harbor Agreement". The Commission Decision 2000/520/EC[281], based on Article 25(1) of Directive 95/46/EC, certifies that the current EU-US data transfer regime provides an appropriate degree of protection for European citizens whose personal data is transferred to the United States of America.

According to Safe Harbor, if American companies want to legally process personal data that comes from Europe, they must comply with a set of principles. They must, in particular, warn people that their information is being gathered and explain how it will be used. Individuals must have the ability to opt out of storing and transferring their data to third parties. Data transfer to third parties can be carried out only by those parties.

Organizations that follow adequate principles for data security. Fair attempts must be taken to avoid the loss of the information obtained. For the reason for which it has been obtained, data must be valid and accurate[282]. Individuals must be able to view, and correct or erase, information kept about them if it is incorrect.

In Safe Harbor, effective means of implementing these rules are included. They merge the private sector's self-regulation with the oversight of public bodies, specifically the Federal Trade Commission (FTC)[283].

However, according to an annex to Decision 2000/520/EC released by the US Department of Commerce, compliance with these principles may be restricted "to the degree appropriate to comply with the requirements of national security, public interest or law enforcement." These restrictions are themselves "limited to the extent necessary in order to satisfy the overriding legitimate interests

[280] Considering the legal procedure see EuGH, Decision of 6 Oct 2015, C-362/14, MMR 2015, p 753 et seqq. with notes from Bergt
[281] Decision 2000/520/EC, cit.
[282] Ibidem note. 280
[283] Ibidem

promoted by such authorization.[284]" In other words, the privacy of EU citizens' personal data becomes a secondary concern when US intelligence allows US companies to collaborate for purposes of national security. This restriction, while not the only data protection issue, has been the key reason why privacy advocates have targeted Safe Harbor.

In order to resolve the contradictions between American and European legislation on the security of personal data, the Safe Harbor Programme was conceived. It is therefore a compromise approach to the degree that the program aims to address, in some way, the shortcomings found by the European Union in the American Personal Data Protection Law, without needing any new legislative interference[285]. The agreement comes into play whenever personal data protected by the Directive is transferred to a U.S. company or business.
The adherence to Safe Harbor establishes the assumption that the adhering organization has an appropriate degree of protection for personal data, allowing the adhering organization to collect data from EU Member States without facing fines from EU institutions.

Adherence to Safe Harbor is entirely optional, American companies are not obliged to join the program; they may well opt to obtain authorization to transfer data directly from the competent guarantor authorities of the Member States, notably through the use of contractual guarantees or codes of conduct.
In either case, if a company wishes to adhere to Safe Harbor, approval by the Member States is presumed, although it remains a requirement for the adhering company to report the data transfer process to the supervisory authority of the competent Member State.

It was noted in the doctrine that neither a treaty nor an international agreement would constitute Safe Harbor, but that it would be the result of two unilateral actions: the US principles and the Commission's decision on

[284] Annex I to Decision 2000/520/EC, cit.
[285] Wiliam J Long, Marc Pang Quek "Personal data privacy protection in an age of globalization: the UE-EU safe harbor compromise", in Journal of European Public Policy :3 June 2002 325-344

adequacy[286].This means that if the agreement does not operate as it should, the adequacy decision adopted by the European Commission may be reversed.
Likewise, it has been noted that Safe Harbor has a hybrid character in that it is the result of a combination of self-regulation in the American tradition and administrative control in the developed European tradition by a state agency[287].

The Safe Harbor Agreement, in addition to the Principles, consists of a collection of frequently asked questions containing a glossary prepared by the Department of Commerce to provide more detail on the interpretation of the Principles. Thus, it provides a summary of how the promises made by the member firm will be fulfilled in the United States, as well as a memorandum on remedial actions made available to individuals[288].

Membership in Safe Harbor is on a self-certification basis. Self-certification is achieved by sending a letter to the Department of Commerce from the company or company indicating that the company adheres to Safe Harbor or by registering online on the website of the Department. Relevant information should be included in the letter, such as contact details and a description of what the organization does with the personal data that it collects from the EU. A summary of the company's privacy policy, including specifics of where the policy is publicly accessible, its effective date and the name of the contact person handling grievances and requests for access to information, should be included in the self-certification process[289].

---

[286] Stephen J. Kobrin "Safe harbors are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance" in Review of International studies (2004), 30, 11-131

[287] Dorothe Heisenberg, nota 6 p. 74

[288] The FTC is not always the authority responsible. The FTC's primary legal authority comes from section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. Other laws ensure privacy in sectors such as health services, telecommunications or some financial and insurance sectors that are outside the FTC jurisdiction, but are covered by other departments or commissions. For cases brought under the SH Framework by the Federal Trade Commission; see also: C. J. Hoofnagle, Federal Trade Commission Privacy Law and Policy, Cambridge University Press, 2016, on the work of the FTC in data protection.

[289] Communication from the Commission to the European Parliament and the Council on rebuilding trust in EU-US data flows, COM(2013) 846 final, 27.11.2013; communication from

In principle, the Safe Harbor Principles follow those of the Directive.

- Firstly, there is the *Principle of Notice*. That is, the organization must tell customers about the reasons for which information is obtained and how it will be used. In addition, organizations need to clarify how to lodge grievances, the types of third parties to which data may be exposed, and how data subjects may be able to prevent such disclosure. Information must be presented in "a clear and conspicuous language" at the same time that individuals are asked to provide their information or immediately thereafter, but the information must be provided before the firm uses the information for purposes other than those for which it was collected or discloses it to third parties[290].
- Secondly, there is the *Principle of Choice*, that allows an organization to give customers the ability to determine on an opt-out basis whether their personal information can be revealed to third parties or used for purposes other than those previously allowed. In addition, with regard to confidential data, before such information may be revealed to third parties or used for an alternative purpose, the data subject must necessarily "opt in"[291].
- The *onward transfer theory* occurs when the entity that has obtained the data plans to report it to a third party. Under Safe Harbor, after verifying that a third party meets the requirements of the Safe Harbor or the Data Directive or other acceptable data protection measure, the company may disclose collected data to a third party acting as its agent. Alternatively, the organization may enter into a written agreement with a third party to

the Commission to the European Parliament and the Council on the functioning of the SH from the perspective of EU citizens and companies established in the EU, COM(2013) 847 final, 27.11.2013.

[290] COMMISSION DECISION of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce

[291] Ibidem

ensure that the data receiver has at least the same degree of data security as under the Safe Harbor agreement[292].

- However, Safe Harbor companies must "take reasonable precautions" against "loss, misuse and unauthorized access, disclosure, alteration and destruction" of data, according to the *Principle of Protection*[293].
- The *fifth principle relates to "Data Privacy"* and allows the processing of personal data to be applicable to the particular reason for which it was collected. This ensures that the data should not be handled by a corporation in a way that is inconsistent with or incompatible with the purposes for which the data was collected[294].
- The *Access Principle* means that the data subject has the right to access his or her personal data in order to edit, correct or remove incorrect data. However, if the expense is disproportionate to the danger in terms of time and resources to the customer, the company would not be obliged to have such access.
- The *final principle is that of Enforcement*. In order for data protection to be considered effective, Safe Harbor companies will need to put in place effective redress mechanisms for data subjects and make clear the consequences for violating the principles. At a minimum, 'readily available, affordable and independent remedies' should be included in the measures adopted by the firms to allow the subject grievance to be investigated and resolved in compliance with the Principles, including, where applicable, damages. In addition, "follow up" processes should be in place to ensure that the organization is effectively in accordance with the principles[295].

[292] COMMISSION DECISION of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce
[293] Ibidem
[294] Ibidem
[295] Ibidem

Austrian student and privacy activist Maximilian Schrems demanded that the Irish Data Protection Commissioner (DPC) forbid the transfer of personal data to the United States through Facebook Ireland (Facebook having its head office in Ireland). He considered that Internet users were not protected from the interference of US agencies, in particular the National Security Agency (NSA), which had unrestricted access to European citizens' personal data, without the need for a judicial decision to be made. This appeal was denied by the Commissioner, claiming that Facebook was accredited under the Safe Harbour Agreement.

In reaction to the inaction of the Irish DPC, Maximilian Schrems then lodged an application for judicial review before the Irish High Court, citing both Directive 1995/46/EC and Arts 7 and 8 of the Charter of Fundamental Rights of the European Union (on respect for private life and the protection of personal data respectively). In an appeal to the CJEU, the High Court questioned whether the adequacy decision stopped the national supervisory authority from preventing the transfer of data on the basis that privacy was not properly covered. On 6 October 2015, the Grand Chamber of the CJEU released a ruling making it clear that national authorities must retain the right to exercise power, provided that the adequacy decision is not declared invalid. The Court then questioned the validity of the decision and ruled that Article 1 of Decision 2000/520/CE[296] was contrary to the provisions of Article 25, para. 6, Directive 1995/46/CE, in the context of the European Union's Charter of Fundamental Rights. As no review of the US rules was included in the decision, the Commission did not include proof that an appropriate standard of security had been achieved.

[296] Schrems [GC], cit., para. 98. On the Schrems ruling: S. CARRERA, E. GUILD, The End of Safe Harbor: What Future for EU-US Data Transfers, in Maastricht Journal of European and Comparative Law, 2015, p. 651 et seq.; C. DE TERWANGNE, C. GAYREL, Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt Schrems, in Cahiers de droit européen, 2017, p. 35 et seq.; R.A. EPSTEIN, The ECJ's Fanal Imbalance: Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices, in European Constitutional Law Review, 2016, p. 330 et seq.; J.F.M. MARQUES, And [They] Built a Crooked Harbor – The Schrems Ruling and What it Means for the Future of Data Transfers Between the EU and US, in EU Law Journal, 2016, p. 54 et seq.; X. TRACOL, Invalidator Strikes Back: The Harbor Has Never Been Safe, in Computer Law & Security Review, 2016, p. 345 et seq.

Moreover, when faced with new situations, this standard of security had to be periodically re-evaluated. Most definitely, Mr. Snowden's disclosures about the NSA Mass Surveillance Program (PRISM) may be seen as a new case justifying a re-evaluation. The Commission should have responded to the fact that US agencies had generalized access to digital communications material without any external and independent control, and without any specific requirements restricting the number of cases in which access was permitted for purposes of national security. In fact, by this time, the Commission had begun to discuss the issue with the US authorities, but this was not enough to alter the position/ruling of the Court.

The Court's decision was consistent with the previous case law supporting data security, which, after the Charter of Fundamental Rights of the European Union (which included a data protection provision) had become legally binding, was more cautious in the early 2000s[297] and more audacious in the post-Lisbon period[298].Although it led to the "Constitutionalisation" of European law by the CJEU, the Schrems decision triggered a renegotiation of the Safe Harbor laws[299].

4.3. EU-US Privacy Shield Agreement and the Case Schrems II

According to an agreement between EU and US members declared on 2 February 2016, Safe Harbour has been replaced by Privacy Shield. In accordance with EU primary and secondary law, the new regime is intended to protect the transfer of data. On 12 July 2016, the Commission adopted a decision declaring

[297]See for instance, Court of justice: judgment of 20 May 2003, joined cases C-465/00, C-138/01, C139/01, Österreichischer Rundfunk and Others; judgment of 29 January 2008, case C-275/06, Promusicae; judgment of 16 December 2008, case C-73/07, Satakunnan Markkinapörssi and Satamedia.

[298] Court of justice: judgment of 8 April 2014, joined cases C-293/12, C-594/12, Seitlinger and Others; judgment of 13 May 2014, case C-131/12, Google Spain. For a general view, O. LYNSKEY, The Foundations of EU Data Protection Law, Oxford: Oxford University Press, 2015.

[299] S. SAURUGGER, F. TERPAN, The Court of Justice of the European Union and the Politics of Law, cit., pp. 158-179; F. TERPAN, Le constitutionnalisme européen: penser la Constitution au-delà de l'État, in Mélanges en l'honneur du Professeur Henri Oberdorff, Paris: Lextenso, 2015, p. 181.

that an adequate standard of protection as required by Directive 95/46/EC[300] should be maintained by the United States and, in particular, by the Department of Commerce. This adequacy decision was based on one declaration and several letters from the US authorities, reproduced in Annexes 1 to 7[301].

A declaration made by the Department of Commerce setting out the Privacy Shield principles is given in Annex 2. Annexes 3 to 5 include letters which have been sent to the European Commission by the Secretary of State, the President of the Federal Trade Commission, and the Secretary of Transport. Annexes 6 and 7 were drawn up by the Director of National Intelligence and the Assistant Attorney General and sent to the Department of Commerce's senior officials, not to the Commission[302].

Thanks to Privacy Shield, is personal data better protected? To what degree does the current regime comply with Schrems' requirements? We differentiate between three situations that are conceivable. Complete compliance refers to a situation in which the level of security provided by the US authorities is equal to that required by the European Union. Non-compliance is when the new regime is essentially identical to the old one, aside from a formal adjustment (adoption of a new judgment on adequacy). Between these two examples, if the Privacy Shield, while enhancing the level of security of European personal data, remains very far from the criteria set by Schrems, we might have partial compliance.

Legal review of the latest documents reveals that three key changes to the EU-US data transfer regime have been made. First, like Safe Harbour, Privacy Shield is based on a certification system: companies can pass data as soon as they are accredited by the US Department of Commerce. They need to comply with a set of privacy standards to be approved. Although the scheme remains unchanged, private operators of the Privacy Shield are subject to greater

[300] Commission Implementing Decision 2016/1250, cit.
[301] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[302] Telecommunication services were subject to an exception from the Free Trade Commission Act and could therefore not participate in the SH self-certification framework. Transport services participating in the SH were monitored by the Department of Transport.

responsibilities with respect to alerts, data retention restrictions, access privileges, privacy policy ads, etc. The Department of Commerce has the authority to examine and oversee the execution of these obligations.

Secondly, the Department of Justice and the Director of National Intelligence issued written confirmation (annexed to the Decision on adequacy) that access to European data by security agencies would be explicitly restricted and regulated. An annual report will be given by the Commission, together with the Department of Commerce and the European and US data protection authorities[303].

Third, stronger control mechanisms favor EU residents. They are now able to lodge a complaint: 1) against US companies which have 45 days to settle the complaint; 2) against European data protection authorities which can lodge a complaint with the Ministry of Commerce. More indirectly, European citizens are able to make an appeal to the Department of Commerce or, if the latter does not follow through, an alternative mechanism. As regards concerns regarding intelligence agencies, the State Department, currently Mrs. Manisha Singhh, has named an ombudsperson (Under Secretary of State for Economic Growth, Energy, and the Environment)[304].

The Ombudsperson responsible for the cases submitted by the European Data Protection Authorities is considered as independent of the intelligence authorities by the European Commission. On 24 February 2016, the Obama administration adopted, in addition to Privacy Shield, a new statute, the Judicial Remedy Act, under which European citizens would benefit from the same

[303] See Data Protection Directive Article 25 (5): 'At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4 [not adequate level]' and (6) 'The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection [...], by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.'

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

protections granted by the US Privacy Act of 1974 to US citizens. This creation was welcomed by the Commission[305].

However, despite these changes, there are still many significant shortcomings in the security provided by the US authorities[306]. Like Safe Harbour, Privacy Shield does not take into account the Commission's assessment of US data protection laws.

One of the main motivations for the CJEU to declare Decision 2000/520/EC on Safe Harbour illegal was the absence of a proper evaluation. There is ample reason to conclude that the Privacy Shield may also be invalidated, as this major error has not been corrected, and the legitimacy of the new regime remains fragile[307].

In addition, the legal existence of the documents supplied by the US authorities is a matter for debate. The general principles applicable to US businesses are laid down on the basis of a clear declaration by the Department of Commerce, which cannot be treated as a legal requirement. Whether these documents can be seen as international agreements between the EU and the US is also doubtful.

Privacy Shield also poses questions about both the company and security aspects. The commercial aspect of Privacy Shield is affected by at least three forms of shortcomings. The first relates to the manner in which information is

[305] Commission Press Release of 24 February 2016, Statement by Commissioner Věra Jourová on the Signature of the Judicial Redress Act by President Obama.

[306] The Art. 29 Working Party emphasised the remaining shortcomings on 13 April and 29 July 2016, before and after the adequacy decision. See: G. VERMEULEN, The Paper Shield, on the Degree of Protection of the EU-US Privacy Shield Against Unnecessary or Disproportionate Data Collection by the US Intelligence and Law Enforcement Services, in D.J.B. SVANTESSON, K. DARIUSZ (eds), Transatlantic Data Privacy Relationships as a Challenge for Democracy, Portland: Intersentia, 2017.

[307] On this issue, the European Parliament adopted a series of resolutions in which it has repeatedly called for the suspension of SH and urged the Commission to take immediate action to ensure effective data protection in transfers to the USA; see: European Parliament, Resolution of 4 July 2013 on the US National Security Agency surveillance program, surveillance bodies in various Member States and their impact on EU citizens' privacy; Resolution of 12 March 2014 US NSA surveillance program, surveillance bodies in various Member States and impact on EU citizens' fundamental rights, and Resolution of 29 October 2015, follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens.

gathered and circulated. For automatic data collection, no clear rules are enforced. And very few assurances are given with respect to the transfer of as well as the role played by sub-contractors, data to third countries. The second group of shortcomings applies to the degree of defense of rights. Private companies are under no duty to remove personal data when it is no longer needed by them. There is no right for customers to reject the collection of data[308].Third, the mechanisms for complaints remain complicated and there are significant reasons for doubting their efficacy.

As far as the security dimension is concerned, we have already mentioned that the system still relies more on letters from US public authorities than on actual legal obligations. Although the National Intelligence Director's Office declares that it will refrain from gathering large and indiscriminate volumes of data, there is no legal way of ensuring that this statement of intent is upheld. Also, the independence of the Ombudsperson, as she works under the Deputy Secretary of the US State Department, remains a concern[309]. The fact that the Commission stated the independence of the Ombudsperson in its adequacy decision is not exactly a guarantee that this independence will be successful[310].

[308] See comments by D. Solove, 'Sunken Safe Harbor: 5 Implications of Schrems and US-EU Data Transfer', TechPrivacy, 13 October 2015. In his view, while EU countries also engage in widespread surveillance ('so there is some hypocrisy here'), the US attitude of acceptance of this widespread power of government surveillance without substantial recourse to judicial challenges (i.e. the fact that the NSA could engage in massive surveillance and that people could not challenge that surveillance) is an arrogance of power unacceptable to the EU.

[309] Among the first reactions to the Schrems ruling, the Schleswig-Holstein DPA (Germany) issued a position paper on 14 October 2015. As for other DPAs, the Italian Garante ruled that transfers based on its previous authorization were forbidden, while companies were allowed to use other tools (i.e., SCC and BCR, as well as specific Garante authorizations). The Spanish DPA (AEPD), required companies operating in Spain to make sure that alternative mechanisms were implemented for data transferred to the USA, warning them of possible enforcement actions if they failed to adopt and notify these mechanisms to the same AEPD. A similar position was taken by the French CNIL.

[310] On the mutual references in the ECtHR and CJEU case law see F. Bohem, 'Assessing the New Instruments in EU-US Data Protection Law', EDPL 2/2016, who also stresses the increasing interconnection between law enforcement and pure surveillance contexts in the USA and EU (with data exchanged between agencies of different sectors), that seems reflected in the lack of distinction made by each court when referring to the other court's arguments. See also Fundamental Rights Agency report, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU', 2017. The CJEU is therefore expected to also apply the same reasoning of the ECtHR in future when assessing the validity, under the CFR, of other EU and Member State legislative acts in this same field.

In its decision of 16 July 2020 "Schrems II", the Court ruled null and void Decision 2016/1250 in which the EU Commission certified the adequacy of the personal data protection provided by the Privacy Shield for EU-US transfers[311]. In short, according to the Court, U.S. domestic laws on access to and use of data transmitted from the EU by U.S. authorities do not comply with the concepts underlying the GDPR, including the concept of proportionality, since there is a possibility for U.S. public and supervisory authorities to access and process personal data transferred without restriction to what is strictly necessary for supervisory reasons[312].

In practice, the impairment found by the Court represents the lack of effective rights of the persons concerned in relation to the US authorities. In that regard, the Court found, inter alia, that the Privacy Shield ombudsman system does not effectively provide protections equal to those needed by EU law, such as ensuring the ombudsman's independence and the existence of rules granting the

[311] Two main aspects of the CLOUD Act stand out: first, the ability of the US government to compel tech companies to disclose the contents of communications stored in servers in foreign countries. To this end, the act amended the Stored Communications Act, as part of the Electronic Communications Privacy Act (ECPA), to compel companies to provide communications data in their control pursuant to warrants of US courts, regardless of whether data are stored inside or outside the USA. In a recent case, Microsoft refused to disclose contents of an email stored outside the USA (in Ireland) and the dispute, before the Supreme Court (in United States v. Microsoft), was declared resolved in April 2018 after Congress passed the CLOUD Act. As for the second aspect, the CLOUD Act authorizes the US government branch to conclude international agreements through which selected countries can access data directly from US companies for prosecution of crimes. Before the Cloud Act, foreign countries were required to use mutual legal assistance or letters of rogatory mechanisms, and the related requests reviewed by US courts for authorization. The act provides that data requests do not target US persons and requires that the foreign country has adequate law and procedures to protect civil liberties (to be assessed by the executive branch). While some observers praised it as a new form of cross-border data sharing, and a practical remedy to demands for evidence stored overseas in criminal cases, others criticize it for the risks it poses to civil liberties and rights by avoiding requirements previously necessary to obtain evidence. Congress can block (within 180 days) a proposed agreement from entering into force by enacting a joint resolution. See S. P. Mulligan, Cross-Border Data Sharing under the CLOUD Act, CRS Report, 23 April 2018 and Lexology.com 'Congress Passes CLOUD Act to Facilitate Law Enforcement Access to Overseas Data'.

[312]The EP's LIBE committee also started in June 2018 a series of hearings to better understand the impact of the Facebook/Cambridge Analytica case, after Mark Zuckerberg (Facebook's CEO) met the EP's President and the political group leaders in Brussels. Moreover, the Shield was also one of the topics discussed by a delegation of MEPs in a visit to Washington from 16 to 19 July 2018.

ombudsman the power to take decisions which are binding on the intelligence services and other public authorities of the United States[313].

Thus, in summary, the Schrems II decision has:

- The Privacy Shield Decision annulled
- Confirmed the validity of the SCC Decision, stating, however, that it imposes a duty on the data exporter and importer to check, by audit/due diligence prior to any move, if, in the third country concerned, a standard of security substantially similar to that guaranteed by the GDPR in the European Union is respected.
- In legitimizing transfers to the United States, the normal contractual provisions have been made ineffective, at least for recipients/importers who are subject to the surveillance systems mentioned in the judgment[314].

With respect to that last argument, the legal team working with Maximillian Schrems in the long court battle that led to the decision under review that most U.S. cloud service providers are subject to controls under FISA Section 702 should be considered - as also correctly pointed out by Noyb, since the same applies to 'electronic communication service providers,' which include[315]:

- Remote computing systems suppliers,

[313] The EU and Japan concluded a deal on reciprocal adequacy of data protection systems in July 2018, which will be followed by a Commission adequacy decision in autumn. The EP's LIBE committee had visited Tokyo in November 2017 in view of its future assessment of the adequacy decision. Its focus was on the negotiations that the Commission had launched with Japan on data transfer in parallel to negotiations conducted on a trade deal with Japan (signed in July 2018). See also G. Greenleaf, 'Questioning 'adequacy' (Pt I) –Japan', Privacy Laws & Business International Report, (2017) 150, 1.

[314] In this case, an adequate level of data protection should be ensured for companies to be able to make EU-UK data transfers. On Brexit and EU rules on data protection see European Commission, Notice to Stakeholders, 9 January 2018. However, there are several reasons to believe that the UK will abide by European data protection rules (see UK Information Commissioner's declaration), so enactment of an adequacy decision to allow EU-UK data flows could be not too difficult. See also C. Kuner, 'The global data protection implications of 'Brexit'', International Data Privacy Law, 2016, vol 6, No 3 and E. Ustaran, The future of international data transfers, Privacy & Data Protection Journal, 2018, Vol. 18, No 6.

[315]Commission Staff Working Document: The application of Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland.

- ❖ Electronic communication services provider,
- ❖ Carriers of Telecommunications,
- ❖ Any other provider of communication services which has access to wire or electronic communications is transmitted or stored either as such communications or as such communications, and
- ❖ Any officer of any other agency, employee, or agent[316].

Considering that, in practice, the transfer of personal data to the United States is primarily based on the adherence of importers to the Privacy Shield or to standard contractual clauses, and that the judgment does not address the question of binding corporate rules.

In the same way as SCCs, it seems to make them useless for transfers to the U.S. It is easy to see how the Schrems II decision has rendered it almost difficult in practice to transfer data to the U.S., at least in the vast majority of situations, that is, where the importer is an "electronic communication service provider[317]".

[316]Federal Data Protection and Information Commissioner press release: After the Safe-Harbor judgment: information on data transfers to the USA.

[317] The EP's LIBE committee also started in June 2018 a series of hearings to better understand the impact of the Facebook/Cambridge Analytica case, after Mark Zuckerberg (Facebook's CEO) met the EP's President and the political group leaders in Brussels. Moreover, the Shield was also one of the topics discussed by a delegation of MEPs in a visit to Washington from 16 to 19 July 2018.

Chapter 5: The "Right to Erasure" between the European Union and the United States of America

The frequent changes identified by the rapid development of information technology call for the jurist to represent and invest in the law of specific duties. The new Regulation 2016/679 of the European Parliament and of the Council on the processing and free movement of data, whose title, not coincidentally, refers not to "personal data protection" but explicitly to "the protection of individuals with regard to the processing of personal data" is a sign of the law's focus on the effect of technology on the lives of citizens[318].

As a result, fundamentally new ideas have arisen, such as cyber surveillance[319], virtual land, virtual currencies[320] and the presence of virtual personas[321].The right to be forgotten from the viewpoint of society represents a natural move forward in a rapidly digitalizing age that poses new challenges that alter the way people view the environment in which they live.

For two key factors, this matter became of absolute significance from the viewpoint of the people. First, as for the largest majority of those living in developing countries, it has shifted from a profit, a must, or even a requirement to be present online[322]. Online platforms have built features that have rapidly become irreplaceable. A Facebook profile, a blog or a YouTube list of interests have quickly become indispensable elements of the lives of people. Not only

[318] S. RODOTÀ, Il mondo nella rete. Quali i diritti, quali i vincoli, Roma-Bari, Laterza, 2014; A. ROUVROY, "Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data, Council of Europe, Directorate General of Human Rights and Rule of Law, vol. T-PD-BUR(2015)09REV, 2016, http://works.bepress.com/antoinette_rouvroy/64/.
[319] David Lyon, *The Electronic Eye: The Rise of Surveillance Society - Computers and Social Control in Context* (1st, Polity Press, 1994).
[320] Joshua Fairfield , 'Virtual Property' [2005] Boston University Law Review 1047. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=807966> accessed 12 March 2015.
[321] Benjamin Guttmann, *The Bitcoin Bible: All you need to know about bitcoins* (1st, BoD – Books on Demand, 2013).

[322] It is a benefit for the multiple advantages it brings, such as permanent connection to news and updates from friends, or access to online books and articles. It has become a must, as enjoying from all these benefits is a necessity in order to remain competitive on the jobs market. It has become an obligation for those who work on digital marketing or PR.

because of the freedom of identification and speech[323], but also because of the need to remain competitive in the social market[324], where people create virtual identities[325] to sell themselves to other people, their online profiles have become part of their persona[326], which is something significantly difficult to give up on. In addition, being online provides invaluable benefits to individual[327]s, such as substantially greater access to employment and job opportunities or easier access to knowledge and information. No pressure can be put on users to willingly choose to opt out of the online world just to avoid privacy risks, considering the value of these benefits for users and for society as a whole. Alternatively, online presence should be embraced in a positive way as a given of the twenty-first century, and thus approached accordingly.

Secondly, in a Big Data environment[328] that goes far beyond the online world, people are forced to work. When governments choose to use more and more modern technology to meet their obligations, people are required to obey their policies and to deal with their consequences. A individual implicitly agrees to give up on his or her privacy, even outside the online world, by becoming a citizen or at least living in a specific country. These situations are when individuals[329] become part of government databases containing personal data,

---

[323] Mitja D. Back, Juliane M. Stopfer, 'Facebook Profiles Reflect Actual Personality, Not Self-Idealization' [2010] Psychological Science.

[324] Joan Morris DiMicco, David R. Millen, 'Identity management: multiple presentations of self in facebook' [e.g. 2005] GROUP '07 Proceedings of the 2007 international ACM conference on Supporting group work 383.

[325] Brian Solis, Deirdre K. Breakenridge, *Putting the Public Back in Public Relations: How Social Media Is Reinventing the Aging Business of PR* (1st, FT Press, 2009).

[326] Craig Ross, Emily S. Orr, Mia Sisic, Jaime M. Arseneault, Mary G. Simmering, R. Robert Orr, 'Personality and motivations associated with Facebook use' [2009] Computers in Human Behavior 578.

[327] Joseph B. Walther, Brandon Van Der Heide, Sang-Yeon Kim, David Westerman, Stephanie Tom Tong, 'The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep?' [2008] Human Communication Research 28.

[328] In the sense that more and more industries are using big data for business purposes: "Big data refers to the idea that society can do things with a large body of data that that weren't possible when working with smaller amounts." The economist, 'The backlash against big data' (economist.com 2014) <http://www.economist.com/blogs/economist-explains/2014/04/economist-explains-10> accessed 20 April 2014. *See also* Linda Frederiksen, 'Big Data here: Big Data' [2012] Washington State University Vancouver.

[329] This might be the case in the US, if such a measure was to be adopted: Julia Angwin, 'U.S. Terrorism Agency to Tap a Vast Database of Citizens' (wsj.com 2012).

when they are subject to workplace surveillance[330], or when they have no option but to be watched on a regular basis on the streets.

Together, governments and courts responded rapidly trying to find solutions to these newly born issues, often effectively, but mostly without a clear vision and knowledge of what is really going on and what the consequences are. This has led to many other issues, such as a lack of uniformity in the rulings of the courts, various, even conflicting views adopted by the Governments, and a general lack of predictability for businesses and consumers alike.

5.1. The "Right to be Forgotten" in the EU context: Legal framework and implementation

Since the historical archives of the media have been digitized and indexed, the public visibility of people (of their image, their prestige, their identity) has become a significant issue, making knowledge about even very old facts readily accessible to web users, thereby deciding an uninterrupted attention to the protagonists.
It is not only considered as fulfillment of the request that such news or data relating to or relating to events legitimately reported in *illo tempore* and relevant to which a fair period of time has elapsed are not published. However, as contextualization, exact reconstruction of human identity, it also imposes itself.

When Viviane Reding revealed that one of the key elements of the GDPR draft was the implementation of the right to be forgotten, she identified the idea as an extension of established privacy rights, indicating that the Data Protection

<http://www.wsj.com/articles/SB10001424127887324478304578171623040640006> accessed 12 February 2015
[329] Serge Gutwirth, Ronals Leenes, Paul de Hert, Yves Poullet, *European Data Protection: Coming of Age* (1st, Springer, 2013) 35-37
<http://www.wsj.com/articles/SB10001424127887324478304578171623040640006> accessed 12 February 2015
[330] Serge Gutwirth, Ronals Leenes, Paul de Hert, Yves Poullet, *European Data Protection: Coming of Age* (1st, Springer, 2013) 35-37

Directive[331] was already setting up the premises for the establishment of such a right.

The natural query that follows is, therefore, whether the Data Protection Directive already provides a right to be forgotten. The importance of this issue is paramount, given the role of the Directive as a benchmark in the harmonization process at EU level, which is being slowly transposed into the legislation of every Member State. Admitting the introduction of such a right would put the pressure on States to accept that persons have the right to be forgotten, thus requiring that laws be immediately rectified.

Specifically, there is an interest in two articles: Article 12(b) and Article 14. The former notes that the right to request data collectors' correction, "erasure or blocking of data the processing of which does not comply with the requirements of this Directive", as applicable, must be given to individuals, in particular where the data is 'incomplete' or inaccurate. Several conclusions may be made using a literal interpretation.

Firstly, this privilege occurs only with respect to data collectors: it does not include third parties or distributors of information. In the context of the debate on information ownership or information autonomy, this is of considerable significance. It effectively rejects the general nature of control over personal data by admitting it as an exception, not as a norm. Secondly, the details must be incorrect or incomplete[332], but not limited to that. This obviously points out a large number of possible scenarios, such as the case of Mr. Costeja, where the reported details were both complete and correct. The findings would be vague and unclear if other parameters were to be considered. Or, provided that no other explicit requirements are expressly referred to in the article, any criteria that would contribute to a case-by-case interpretation may be treated as being protected. Third, this refers to the processing of data, including, though not

[331] Being specifically named as one of the "four pillars" of the new Regulation, according to the press release. Mitchel-Rekrut (n.112) 3.

[332] Article 12 states "in particular because of the incomplete or inaccurate nature of the data" which suggests that others cases may be considered as well.

limited to, the compilation and storage of such data[333].It must therefore be combined with the provisions of Article 6 (the requirement of 'equal' and 'legal' processing) and Article 7 (the necessity of 'fair' and 'legal' processing) (criteria used to assess the legitimacy of data processing, such as consent and necessity of processing).

Article 14 states that persons have the right to object, at least but not limited to the cases referred to in Article 7(e) and to the cases referred to in Article 7(e) and to the cases referred to in Article 7(e) at any time on compelling legitimate grounds relating to their particular circumstance, to the processing of data relating to them, except where otherwise provided for in national legislation (f). This means that first of all, the data owner must have "compelling legitimate grounds" for objection, which violates the concept of possession of information which some consider to be the foundation of the right to be forgotten. Furthermore, it is not clear what "object" means and whether this has functional implications, such as the right to request the deletion of data. Finally, this rule is not imperative: Member States can provide otherwise, rendering in at least some cases this right to object inefficient.

With this general broad structure in mind, some States have agreed to adhere to the restrictions found in the Directive, while others, as in the case of Article 14, have minimized it wherever possible. Other Member States, such as the national data protection agencies[334] of Italy, Spain and France, have agreed to go one step further, implementing a more protective legislative framework which specifically recognizes the existence of a right to be forgotten. In all instances, their attempts have departed from these two papers, which admittedly contain some, albeit poor, version of the individual's possible right to control his or her own data.

[333] Article 2(b) states that 'processing' means any operation or set of operations carried out on the basis of personal data, whether or not by automated means, such as compilation, recording, arrangement, storage, adaptation or modification, collection, consultation, use, disclosure by means of transmission, dissemination or otherwise making available, alignment or combination.
[334] Other Member States, such as the national data protection agencies of Italy, Spain and France, have agreed to go one step further, implementing a more protective legislative framework which specifically recognizes the existence of a right to be forgotten.

It is definitely correct to claim that the extent and limitations of every right, including the right to be forgotten, are ultimately related to the issue of jurisdiction, but that is a real Internet problem. Evidence of this is the fact that the providers who operate the search engines have appealed to the European Courts in many instances. In fact, this rebounds in competences once again risks neutralizing the efficacy of the discipline at issue, specifically the European discipline. Certainly, exempting a kind of territoriality principle is not the best way to look for a solution to the problems faced, even though it is a compromise.

This presents a possible tension between various rights: on the one hand, freedom of speech, the right to publish news, the right to know; on the other hand, the right of the subjects participating in the news to exert control over the information that affects them directly, restricting their exposure to the web for a limited period of time.

The controversial concept of the right to be forgotten, interpreted as the right of the person concerned to receive the withdrawal from public circulation of personal information relating to him or her, at the crossroads of all these topics, where its public importance has decreased due to the passage of time or for other reasons, has arisen over the last few years in the sense of a jurisprudential and doctrinal level[335].

[335] A.L. VALVO, The right to be forgotten in the age of "digital" information, in European Integration Studies, 2015, no. 2, pp. 347-358; E. CRUYSMANS, C. ROMAINVILLE, Les diverses dimensions du "droit à l'oubli" Lextenso éditions, 2015, pp. 81-92; P. KORENHOF, J. AUSLOOS, I. SZEKELY, M. AMBROSE, G. SARTOR, R. LEENES, Timing the Right To Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data, in S. Gutwirth, R. Leenes, P. de Hert (eds.), "Reforming European Data Protection Law," Springer, 2015, pp. 171-202; C. MARKOU, The 'Right To Be Forgotten'. Ten Reasons Why It Should Be Forgotten, ibid, pp. 203-226; G. ZANFIR, Tracing the Right To Be Forgotten in the Short History of Data Protection Law. The "New Clothes" of an Old Right, ibid, pp. 227-252; F. DI CIOMMO, Quello che il diritto non dice. Internet and oblivion, in Danno e responsabilità, 2014, no. 12, pp. 1101-1113; F. PIZZETTI (ed.), Il caso del diritto all'oblio, Torino, Giappichelli, 2013; V. MAYER-SCHÖNBERGER, Delete. Il diritto all'oblio nell'era digitale, Milano, Egea, 2013; G. FINOCCHIARO, La memoria della rete e il diritto all'oblio, in "Il diritto dell'informazione e dell'informatica", 2010, n. 3, pp. 391-410; M. MEZZANOTTE, Il diritto all'oblio. Contributo allo studio della privacy storica, Napoli, Edizioni Scientifiche Italiane, 2009; D. MESSINA, Le prospettive del diritto all'oblio nella società dell'informazione e della comunicazione, in questa Rivista, 2009, n. 1, pp. 93-103.

It is expressly alluded to in Article 17 of the new Regulation 2016/679: *"Right to erasure"* or the *"Right to be forgotten".* In compliance with paragraph 1 of that clause, the data subject's right to obtain from the data controller the erasure of personal data relating to him or her and the related duty of the data controller to delete the personal data relating to him or her, provided that one of the following conditions:

- That the data is no longer relevant for the purposes of the processing[336].
- The data subject withdraws his or her consent to the processing and no other legal reason exists for the processing[337].
- The data subject is objecting to the processing and no other legal justification exists for the processing[338].
- Data has been illegally processed[339].
- A legal duty exists to delete the data[340].
- Data were obtained in connection with the provision of services to minors in the information society[341].

In the same way, Article 17 illustrates the possible conflict between that right and other constitutional rights: the situations in which there is no right to cancel, or corresponding duty are actually indicated in paragraph 3, because data processing is necessary:

- For the exercise of the right to freedom of speech and of information[342].

[336] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation

[337] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation

[338] Ibidem

[339] Ibidem

[340] Ibidem

[341] Ibidem

[342] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- For the performance of a legal duty or for the performance of a mission performed in the public interest or in the exercise of official powers to which the data controller is assigned[343].
- In the area of public health for reasons of public interest[344].
- For archiving purposes in the public interest, for scientific or historical analysis or for statistical purposes[345].
- In order to create, exercise or defend legal claims[346].

While the right to be forgotten derives from the CJEU's interpretation of the current data protection legislation in 2014, a new development would dramatically shift the debate forward.

Data subjects may have the right to erasure in order to resolve a condition in which one of their specified rights is at risk. The above is explicitly excluded and the new condition that data 'must be correct and preserved up to date' is an important aspect of the existing version of the right to be forgotten found in the decision of Google Spain.

Although the proposed right to delete allows the consumer some more power to object to processing, it might no longer be applicable to the very founding concept behind Google Spain. While it may be simpler to take action, it seems like the need to delete unnecessary detail that makes it easy to forget what it is has been diluted. However, one might argue that the prohibition against unlawful processing also provides the right to object to incorrect and out-of-date records, as it is large enough to allow such action.

Furthermore, Article 17 contains an inbuilt reference to equilibrium with freedom of expression and, for the purposes of 'exercising the right to freedom of expression and information,' paragraph 3 contains an exception to the right to

[343] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation

[344] Ibidem

[345] Ibidem

[346] Ibidem

erasure. Hopefully, much of the above-mentioned critiques that see the right to be forgotten as a potential obstacle to freedom of speech should rest on this. The in-built balance can, however, serve to further dilute the right's influence.

As is well known, the judgment of the European Court of Justice of 13 May 2014 in Case C-131/12, Google Spain vs. Mario Costeja González[347], which sparked a very large debate in scientific circles, technical circles and public opinion, was the one that most referred to the assertion of the right to be forgotten, with particular reference to the operation of search engines on the Internet.

This is the first case in which traditional data security standards explicitly extend to the Internet in a way that allows search data to be erased. The case involves Mario Costeja González, a Spanish national, whose name was listed on the website of La Vanguardia, a Spanish newspaper, describing a real-estate sale linked to the social security debt recovery process. Those pages came up close to the top whenever anyone searched for his name. Mr. Costeja González lodged a complaint with the Spanish Department for the Security of Data (Agencia Española de Protección de Datos, AEPD) using his rights under the Spanish Data Protection Directive transposition. On the basis of Articles 6 and 12[348] of the Data Protection Directive referred to above, Mr. Costeja González demanded that the pages of La Vanguardia be removed or altered and also requested Google Spain to delete or hide the personal data relating to him, so that they would cease to be included in the search results and would no longer appear in the links to La Vanguardia.

[347] Google Spain v Agencia Española de Protección de Datos and Mario Costeja González, case C131/12, 13.05.2014. ECLI:EU:C:2014:317.

[348] JUDGMENT OF THE COURT (Grand Chamber) 13 May 2014 Language of the case: Spanish. (Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8)

The AEPD refused the request in relation to the La Vanguardia newspaper, alleging that the publication of such data was legally justified and that it is a normal practice for the publication of such information in the national press. The AEPD, however, granted the order relating to Google and demanded that the results of the search engine concerning Mr. Costeja González not provide a connection to the infringing sites.

Unsurprisingly, the decision was appealed by Google to the national high court (Audiencia Nacional), which referred a number of questions to the CJEU, requesting clarity as to the application of the Data Protection Directive.
The concern was whether search engines should be considered data controllers and, thus, whether they should provide users with tools to change or exclude incorrect personal data from their listings.

It was determined by the CJEU[349] that:

- Search engines should be known as personal data processing engines and should thus be called data controllers[350].
- As such, search engines are considered to work in the country "for the promotion and sale of advertising" by providing an office, branch or subsidiary[351].
- As a data controller, the search engine is allowed to 'delete from the list of results displayed after a search made on the basis of a person's name links to web sites, published by third parties and containing information

[349] Sentenza della Corte (Grande Sezione) 13 maggio 2014, Google Spain SL, Google Inc. vs. Spanish Data Protection Agency (AEPD), Mario Costeja González, Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN
[350] [350] JUDGMENT OF THE COURT (Grand Chamber) 13 May 2014 Language of the case: Spanish. (Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8)
[351] Ibidem

related to that person,' even though the information displayed on that page is valid[352].

- ❖ When analyzing a data subject's request to remove links to a search result, authorities should balance the interest of the subject in accordance with her rights under the European Convention on Human Rights, the economic interest of the service provider, the role played by the data subject in public life, and the public's interest to have access to the information[353].

Therefore, as addressed so far in the CJEU judgment of 13 May 2014, the right to be forgotten has been acknowledged within the EU, without, however, having reached a strong and specific indication in this regard as to how to implement it.

5.2. How the "Right to be Forgotten" in the U.S. violates the 1 Amendment of the U.S. Constitution

The United States was caught in the midst of a huge effort to resolve privacy matters following the CJEU decision and the events that followed, as well as other privacy-related changes taking place worldwide[354]. The US system was challenged when the European Union announced its intention to implement "more effective and standardized data privacy laws across Europe"[355]. The wider discussion about precisely where the line between the right to privacy and freedom of expression should be drawn was essential to the interpretation and

[352] Ibidem

[353] JUDGMENT OF THE COURT (Grand Chamber) 13 May 2014 Language of the case: Spanish. (Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8)

[354] 'Everyone is under surveillance now, says whistleblower Edward Snowden' (theguardian.com 2014) <http://www.theguardian.com/world/2014/may/03/everyone-is-under-surveillance-now-says-whistleblower-edward-snowden> accessed 15 March 2015.

[355] Dawinder Sidhu, 'We Don't Need a "Right to Be Forgotten." We Need a Right to Evolve.' (newrepublic.com 2014). <http://www.newrepublic.com/article/120181/america-shouldnt-even-need-right-be-forgotten> accessed 18 March 2015.

evaluation of the right to be forgotten. While the European approach was criticized by some, others accepted its adequacy and thus advocated for a similar strategy.

For a long time, the US vision of privacy and personal data has contradicted the European view. While the general vision of the EU Member States is to concentrate on the citizen and his rights, to justify state interference in order to ensure the security of the public person[356], the United States implements a market-oriented approach, with voluntary codes of conduct[357], to establish a less centralized legislative structure, with subject-specific rules aimed at minimizing state intrusions[358]. Europe considers personal data to be an important part of the identity of an individual, being more likely to recognize a right to be forgotten, whereas the United States is known to have a strong preference for disclosure, often giving less weight to privacy than to interests that are more "appropriate to protect", such as national security[359].

In this context, the fundamental aspect of the debate on privacy versus freedom of expression is whether or not there is a right to be forgotten in the US, specifically with regard to the resolution of disputes that their dispute might entail, as well as with regard to restrictions that the state is allowed to enforce on the right to privacy and how effective it is to protect the rights of its people. There is one thing that is obvious, regardless of the result of this debate[360]: the

[356] James Daley, 'Information Age Catch 22: The Challenge of technology to cross-border disclosure & data privacy' [2011`] Sedona Conference Journal 6.
[357] Joel R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' [1999-2000] Stanford Law Review 1316.
[358] Daley (n 151) 6.
[359] The case of the mass surveillance conducted by the NSA, which has been largely analyzed by both scholars and media. *See* Joseph D. Mornin, 'NSA Metadata Collection and the Fourth Amendment' [2014] Berkeley Technology Law Journal 984 or Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' [2014] Fordham Law Review 2136 or Ilina Georgieva, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' [2015] Utrecht Journal of International and European Law 104

[360] Hayley Tsukayama, ''Right to be forgotten' highlights sharp divide on U.S., European attitudes toward privacy' (washingtonpost.com 2014) <http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/13/right-to-be-forgotten-highlights- sharp-divide-on-u-s-european-attitudes-toward-privacy/> accessed 20 March 2015.

official acknowledgment of the right of its transatlantic neighbor to be forgotten has exposed fundamental weaknesses in American society, triggering harsh reactions on both sides[361]. Eventually, these vulnerabilities will have to be fixed, so state and court action will be required. The introduction of the EU right to be forgotten might just be a legitimate solution in this case. If it leads to evolution or regression, however, only time can tell.

The fact that the United States does not have a right to be forgotten[362] cannot be easily disputed. At least, not in the same way that it is defined by European countries. At the end of the day, the country does not have a consistent, homogeneous federal data security and privacy law system, leaving consumers and users at the hands of corporations or federal states who wish to take action to protect the privacy of their residents.

The defense of US privacy is distributed and distributed through a number of state and federal laws that usually apply to particular classes of people[363]: it is a "patchwork series of laws[364]." In terms of how the same legal problem can be addressed, this necessarily leads to discrepancies from state to state, and field to field.

Given this lack of continuity and homogeneity, to be forgotten is not a total stranger to some variants of this correct. In reality, US law has long-standing experience with "legal forgiveness[365]," a term profoundly impregnated by numerous layers of the legal system.

It has a long tradition of arguing for individual privacy, early in history, at the end of the nineteenth century, when scholars discussed the tension between risks to the privacy of individuals raised by then-modern technologies such as

[361] For an overview on these reactions *see* Sidhu (n 150).

[362] As some authors conclude after analyzing the situation. *See* Karl S. Kronenberger, 'The tension between principles of "Sunshine Laws" and "The Right to be Forgotten": Trends in the treatment of personal information on the internet' [2014] Aspatore: Understanding Developments in Cyberspace Law 2.

[363] Victor Luckerson, 'Americans Will Never Have the Right to Be Forgotten' (time.com 2014). <http://time.com/98554/right-to- be-forgotten/> accessed 19 March 2015.

[364] According to Andy Sellars, a staff attorney for the Digital Media Law Project housed at Harvard University ibid

[365] Ambrose (n 31) 9.

telephone and photography, advocating for the latter in an article that would become a cornerstone of the privacy perspective[366].

Even case law has shown court support for at least the prospect of allegations based on adverse reference to out-of-date information for privacy infringement. Cases such as *Melvin v. Reid*[367] (1931) or *Briscoe v. Reader's Digest Association, Inc*[368] (1971) indicate that American courts have long pondered whether a right to be forgotten should be acknowledged, as the value of forgiveness in one's recovery has been stressed by their argumentation.

While both cases were overruled with a view to safeguarding the freedom of speech guaranteed by the First Amendment, the arguments used by those courts remain a relevant point in the wider debate. However, in the case of matters that are worth the attention of the media, US courts also deny privacy arguments today, unless any specific or extraordinary circumstances exist that would warrant exceptions.

In criminal law, certain situations may arise where reinvention is perceived to be an essential part of the recovery process and is seen as prevailing over the public's right to be aware. The presence of amnesty and limitation status enables people who have completed their sentence to move on without having to bear the weight of their past mistakes[369]. They can regain influence of their lives and participate in constructive activities that can bring value to society by getting their integrity returned after enough time has passed to be deemed to have

[366] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' [1890] Harvard Law Review 193.

[367] In this case, a homemaker who used to work as a prostitute, was accused of murder. Although she was acquitted as the accusations proved to be unfounded, her trial was used as the main subject in a movie made after seven years, her name being used explicitly. The Court considered that the use of her name was inhibiting the process of rehabilitation, an essential element of the penal system. *Melvin v Reid* [1931] 112 285 (Call. App).

[368] In this case, the Court similarly said that rehabilitation may be hinged by the explicit referral to the plaintiff's prior crimes. *Briscoe v Reader's Digest Association* [1971] 4 529 (Cal.3rd).

[369] *See* Tyler T. Ochoa, 'The Puzzling Purposes of Statutes of Limitation' [1997] Santa Clara Law Digital Commons 452.

learned their lesson[370]. Some states, such as Wisconsin[371] or New York[372], also forbid employers from refusing jobs only on the basis of criminal records for convicted convicts; others go further and address the possibility of "postponing background checks until after the preliminary hiring decisions are made"[373].

Finally, the case of California, which has made strides over the last few decades in ensuring adequate security of consumers' personal and private information, should also be listed. In the case of security breaches, its legislative initiatives, such as the California Online Privacy Protection Act of 2003[374], or the more recent changes introduced to California's data breach legislation in 2013[375], place limits on the processing of information and disclosure of information, while some elements remain[376].These rules, as well as other legislative measures, such as the California "Online Eraser" Minors Act, which entered into force on 1 January 2015 and was vehemently challenged[377], reflect

[370] For why reputation is an important element in people's lives and why it can be easily affected in the online environment, *see* Hassan Masum, Mark Tovey, *The Reputation Society. How Online Opinions are Reshaping the Offline World.* (1st, The MIT press, Cambridge, Massachusetts 2011).

[371]Article 111.321 states that "no employer, labor organization, employment agency, licensing agency, or other person may engage in any act of employment discrimination as specified in s. 111.322 against any individual on the basis of (…) arrest record, conviction record (…)". Wisconsin Fair Employment Act 2000 s 111.321.

[372] Article 752, called "Unfair discrimination against persons previously convicted of one or more criminal offenses prohibited" states that "No application for any license or employment, and no employment or license held by an individual, to which the provisions of this article are applicable, shall be denied or acted upon adversely by reason of the individual's having been previously convicted of one or more criminal offenses (…) when such finding is based upon the fact that the individual has previously been convicted of one or more criminal offenses (…).".New York Correction Law 1995 s 752.

[373] Ambrose (n 31) 9; This is the case of the New Mexico Statute Annotated 2010 28(2-3B) or Hawaii Revised Statute 2010 s 378(2).

[374] Scott Allen, 'California Online Privacy Protection Act of 2003 — Good Practice, Bad Prece' (about.com 2014) <http://entrepreneurs.about.com/od/internetmarketing/i/caprivacyact.htm> accessed 13 March 2015.

[375]Updating its breach notification requirements and making it the first state to expand the definition of personal information to expressly include login credentials for online. Adnan Zulfiqar, 'California Expands Breach Notification Law to Cover Online Accounts' (hldataprotection.com 2013) .<http://www.hldataprotection.com/2013/11/articles/cybersecurity-data-breaches/california-expands-breach-notification-law-to-cover-online-accounts/> accessed 13 March 2015.

[376] *See* Kronenberger (n 157) 2.

[377] Thomas R. Burke, Deborah A. Adler, Ambika K. Doran, Tom Wyrwich, ' California's "Online Eraser" Law for Minors to Take Effect Jan. 1, 2015' (dwt.com 2014)

an approach comparable to that adopted by European counterparts, albeit still raw.

In the US method, therefore, there is a right to be forgotten: it may be present in a sketchy or fragmentary edition, but the main concept is present. This can be clarified because the notion of "forgive and forget" is considered, as some scholars[378] have noted, to be an intrinsic part of human nature and is thus legitimately used as a legal system principle[379].Thus, its role in many of the American political decisions, one of the world's most fierce advocates for human freedoms, is rightly justified.

For years, the United States has contemplated the effect and significance of the concept of "forgive and forget" and sometimes even applied it as it deemed necessary. As previously seen, US culture has the grounds for a right to be forgotten, as an embryonic version of it is in fact already known in some instances. Having identified that, it is important to ask another critical question: should there be a right to be forgotten which is identical to the one which the EU has been trying to implement?

Two important aspects need to be studied to address this issue. Second, if the legal system currently in place will allow a right to be forgotten to be exercised. This will include analyzing the First Amendment and the Decency Act on Communications.

<http://www.dwt.com/Californias-Online-Eraser-Law-for-Minors-to-Take-Effect-Jan-1-2015-11-17-2014/> accessed 18 March 2015.

[378]Bennett (n 46) 2.

[379] "Since the beginning of time, for us humans, forgetting has been the norm and remembering the exception", the author further arguing that the recent technological developments led to paradigm shift whose potential need for correction should at least be analyzed. Mayer-Schönberger (n 97) 2.

The major concern lies in the incorporation of all that is posted online under the safe harbor of "free speech," which is protected by the First Amendment.

The First Amendment, claiming that:

"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."

It is a pillar of American democracy and represents the public's interest in receiving the requisite information for informed self-government[380], as well as the complementary interest of the press in supplying the public[381] with accurate and valuable information. Censorship[382] can be seen as any effort to curtail this freedom of speech, contributing to massive public outrage.

Although it extended its reach with time, the defense of the First Amendment was originally meant to include the disclosure of government data regarding other persons, such as court rulings, judgments, records, summaries of what has occurred in the past: essentially, all official government documents should be released, with few exceptions, such as social security numbers[383].

Today, however, the defense of the First Amendment is primarily aimed at covering the free expression of individuals and private companies on the market. It is now considered that the First Amendment also includes the

[380] Beyond states' interest to have informed citizens in order to make informed democratic decisions, there is a question on whether citizens have a right to be informed. *See* Natalie Helberger, *Controlling access to content. Regulating Conditional Access in Digital Broadcasting* (1st, Kluwer Law International, The Netherlands 2005) 89. Talking about pay-TVs, the author states that the public generally does not have a right to access information: "The right of the public to be properly informed has to be read within the context of the task that the media have to perform".

[381] As explained here Alan M. Katz, 'Government Information Leaks and the First Amendment' [1976] California Law Review 108.

[382] Matt Ford, 'Will Europe Censor This Article?' (theatlantic.com 2014) <http://www.theatlantic.com/international/archive/2014/05/europes-troubling-new-right-to-be-forgotten/370796/> accessed 19 March 2015.

[383] Kronenberger (n 157) 3.

compilation of results they provide ‚Langdon v. Google[384], due to the essence of the function of search engines: The definition by Google of the system it uses shows "the inherent subjectivity of how results are compiled,[385]" using parameters such as consistency, popularity or significance[386] in website judgment. For example, by determining how many other websites connect to the analyzed website, algorithms such as PageRankTM evaluate the popularity of websites.

Even if this defense is justified by the subjective nature of its operation, the question is whether it is reasonable to apply any kind of restriction. Under the First Amendment, freedom of expression is not an absolute right[387]. It is possible to ban[388] some forms of speech, with certain types of speech being more easily limited than others[389]. In case law, an answer can be sought. Some decisions have agreed that, in some cases, access to information can and should be limited. The Supreme Court agreed in the US Department of *Justice v. Reporters Committee for Freedom of the Press* that the "compilation of otherwise difficult-to-obtain information" that "would certainly have been forgotten otherwise" would improve its visibility, generating unjustified challenges to the "privacy interest in maintaining the practical obscurity of the information.[390]"

The Supreme Court, in *Nixon v. Warner Communications, Inc*., emphasized the duty on courts to ensure that public access to information is not provided for

---

[384] In this case, the court found that search results constitute speech under the First Amendment, and that Google, Yahoo and Microsoft are immune with regards to their editorial decisions regarding screening and deletion from their networks. See a thorough analysis here: Martin Samson, 'Christopher Langdon v. Google Inc., et al.' [2007] Internet Library of Law and Court Decisions.

[385] Haynes Stuart (n 127) 6.

[386] James Grimmelmann, 'Speech Engines' [2014] Minnesota Law Review 868.

[387] Bennett (n 46).

[388]"Restraints on free expression may be permitted for appropriate reasons" as "Speech often hurts", invoking Elrod v. Burns [1976] 427 347 (U.S.). Geoffrey R. Stone, Louis M. Seidman, Cass R. Sunstein, Mark V. Tushnet, Pamela S. Karlan, *The First Amendment* (4th, Wolters Kluwer Law & Business, 2012) 3, 8.

[389] These articles analyze some areas in which the freedom of speech may be restricted. *See* Kathleen Ann Ruane, 'Freedom of Speech and Press: Exceptions to the First Amendment' [2014] CRS Report for Congress or Alan M. Katz, 'Government Information Leaks and the First Amendment' [1976] California Law Review 108.

[390] *DOJ v. Reporters Comm. for Free Press* [1989] 489 749 (U.S.).

"improper purposes," such as the fulfillment of private spite or the promotion of public scandal[391]. The same vision was shared by some scholars, who recognized that "even in the current age, when information is king, the soundest policy choice is sometimes less access to information[392]".

Both of these demonstrate that the American legal system is prepared to embrace a balance between, on the one hand, the right to access information and freedom of expression and, on the other, the right to privacy and to protect personal identity. Thus, the only prerequisite for the right to be forgotten to be recognized as legitimate under the First Amendment would be a sufficient, detailed and persuasive argument as to why the freedom of expression of search engines should be superseded by the interest in preserving privacy.
Given that such claims already exist, this would not be something too difficult to imagine[393]. Alternatively, search results posted by search engines such as Google may begin to be viewed as commercial expression, putting them in an intermediate category that would require less constitutional protection[394].

A remarkable decision in the history of data security was taken by the CJEU. By officially accepting the presence of the right to be forgotten in the EU legislative context, it clarified the role that the EU market should take in relation to personal data and privacy, the implications of which are essential to the evolution of the rules on privacy. In addition, the constitutional and ideological structure of the United States is consistent with the way the EU has approached the nature of the right to be forgotten. Consequently, if such technological and institutional hurdles are resolved, the transition to a more privacy-friendly legal system, ready to recognize the right to be forgotten, may be feasible.

---

[391] *Nixon v. Warner Communications, Inc.* [1978] 435 589 (U.S.).
[392]Daniel J. Solove, 'The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure' [2003] Duke Law Journal 967.

[393] See 'The U.S. Should Adopt The 'Right To Be Forgotten' Online' (intelligencesquaredus.org 2015) <http://intelligencesquaredus.org/debates/upcoming-debates/item/1252-the-u-s-should-adopt-the-right-to-be-forgotten-online> accessed 18 March 2015.
[394] Haynes Stuart (n 127) 9.

One aspect is apparent, however. If a coherent approach to the life and application of the right is not followed, the contradictions in the vision between the US and EU communities will intensify, contributing both to an intensification of existing problems and to the creation of new ones. In addition to being inconsistent from one jurisdiction to another, the enforcement of laws may transform law into a region of unpredictability and confusion. This would lead to unjustified disparities in the treatment of individuals and private organizations, which would undermine overall trust in the legal system. In order to comply with the inconsistencies, the economy will also be affected, as businesses could be required to take undesired measurements.

Conclusions

Globalization, technological evolution and freedom of communication, if, on the one hand, have been over time drivers of secure development and planetary economic trade, on the other hand, individual privacy protection problems have arisen and, more recently, security and national public order problems have emerged. Collective security considerations are now at the forefront of our latest legal and political experience and are rapidly influencing the growth of political and economic phenomena as well.

The right to privacy coincided with the American *"right to be left alone"* before the technological revolution that allowed the rapid collection, organization and transmission of a set of personal data at the dawn of the dissemination of communication via printed paper. The latter, discovered in the 1890 publication of the essay The Right to Privacy, signed by Samuel D. Warren and Louis D. Brandeis, contributed to the establishment of the notion of protection with the attribution to the person of the right to be left alone, undisturbed, to enjoy, thus, a private domain shielded from outsiders' interference. This U.S. conception of privacy, distinguished by a strict jurisprudential existence, for a long time found citizenship in the European legal world before a redefinition was enforced by technologically advanced society.

In particular, in Europe, after the historical experience of the mass exploitation of personal data by authoritarian regimes, in particular those sensitive ideological and political affiliation data, all abused by systemic manipulation of the oppressive and anti-democratic key. To obtain importance as a constitutionally protected right and, as such, to be protected not only against individuals but also against public power, the need for protection of individuals against interference in privacy was important. The Council of Europe's experience and the European Court of Human Rights' jurisprudence have led to this European idea of the right to privacy. The right to the privacy of personal data was born, so that the provisions of Directive 95/46/EC were initially enforced in a jurisprudential manner and subsequently implemented. Finally, the

same was officially “consecrated” within the scope of an ad hoc clause laid down in Article 8 of the Charter of Fundamental Rights of the European Union, to which the Treaty of Lisbon gave binding power, bringing it to the same standard as other treaties.

Thusly, this recognition separates European law from the legal practices of other Western democracies, such as the United States of America in particular, and is the explanation for its specific importance in the context of legislative security as well. Whereas in Europe, in the general and universal legal system, the protection of personal data determines the purposes of the protection sought by an instrument of general law, in the United States, on the other hand, the Federal Constitution does not specifically refer to the protection of personal data in the list of constitutional rights. The latter is drawn up on the basis of highly sectoral and decentralized regulations, with clear differences between the private and public sectors, where the self-regulation mechanism is in place. Moreover, the current threats brought to Europe by technological progress contribute to the protection of the private sphere from modes of regulation that can be exerted by new technology, through the predisposition of particular regulatory remedies. Thus, after a long evolutionary period, we have progressed from the initial right to privacy to data security, which has declined as a fundamental right of the citizen both within the national and EU legal systems.

Hence, the latest General Regulation on the security of data outside the territories of the Union, as a normal and unavoidable consequence of international commercial transactions and of the interconnectedness of interpersonal ties in the internet age, is not a secondary feature. In this particular matter, the principles regulating the legality of transfers of personal data to third countries under European law have already been identified and the regulatory mechanisms available to the European Union in this area have been examined. All of this with the aim of ensuring an appropriate degree of security for the transfer of personal data, which today appears to be one of the real foreign policies of the European Union, aimed at ensuring a high standard of protection

for European citizens' data, regardless of their residence, in the sense of international relations with third countries. The Privacy Shield Agreement aimed to protect the security of the data of European citizens in the event of data transfer to servers located in the American territory, which replaced the previous Safe Harbor Agreement, after the European Court of Justice's censorship pronouncement. It was an effort, with the imposition of tougher obligations, to provide better security for American companies processing European citizens' data by means of a very strict control and monitoring mechanism put in place by the authorities of the European Union.

In this new context, the subject of the Right to be Forgotten is implemented, aimed at ensuring that the person has total control over his own information. The likelihood that the Institute of the Right to be Forgotten gives the interested party the power to erase signs of its own history, potentially undermining the exercise of the right to know, has, in the judgments expressed at European and American level, produced various contrasts. In conclusion, it should be remembered that the prospect of being able to neutralize a piece of news in the digital mare magnum in an absolute way remains very difficult at the moment, despite the undoubted progress achieved by the elaboration of the Right to be Forgotten by the institute.

Bibliography

Amato F., Sbaraglia G., *GDPR. Package for survival. Knowing it, implementing it and preventing fines for privacy and data collection*, 2018, goWare Content Team.

Anrig G., *The war on Our Freedom: Civil Liberties in an Age of Terrorism*, 2003, Washington, The Century Foundation.

Arendt H., *The origins of Totalitarianism*, 1984, Piccola Biblioteca Einaudi.

Atkinson A. B., *The Fourth Amendment's National Security Exception: Its History and Limits*, 2013, in Vanderbilt L.Rev., 1343, 1381.

Becker M., *Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy*, 2019, Ethics and Information Technology.

Bell H., *The Patriot Act*, 2004, Santa Barbara.

Bloch-Wehba H., *Confronting Totalitarianism at Home: The Roots of European Privacy Protections*, 2015, Brooklyn Journal of International Law, Volume 40, Issue 3.

Blounstein E. J., *Privacy as an aspect of human dignity: an answer to Dean Prosser*, in New York University Law Review, 1964, page. 974

Böhm A., *A comparison between US and EU Data Protection Legislation for Law Enforcement*,
2015, p 69 et seqq.

Brash W. M., *America's Unpatriotic Acts*, 2005, New York.

Cardarelli F., Sica S., Zeno-Zencovich V., *The personal data code. Themes and 44 problems*, 2004, Giuffrè, Milan.

Carrera S., Guild E., *The End of Safe Harbor: What Future for EU-US Data Transfers*,2015, in Maastricht Journal of European and Comparative Law, p. 651 et seq.

Clark Kelso J., California's Constitutional Right to Privacy, 1992, Pepperdine Law Review.

Clarke R., *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, , Original of August 15, 1997, revs. Sep 1999, Dec 2005, Aug 2006, October 21, 2013, July 24, 2016.

Colarocco V., *The transfer of data to third countries, in the process of the GDPR*, edited by G. Cassano, V. Colarocco, G. B. Gallus, F. P. Micozzi, 236.

Coles T. R., *Does the Privacy Act of 1974 protect your right to privacy? An examination of the routine use exemption*, 1991, in American University Law Review, Vol. 40, p957-1002, 46p.

De Hert and Gutwirth, *Data Protection in the Case of Law of Strasbourg and Luxemburg: Constitutionalisation,*2009, Springer.

De Hert P, Gutwirth S., *Privacy, data protection, and law enforcement. The opacity of the individual and transparency of power*, 2002, Arnhem, Kluwer/Gouda Quint.

De Minico G., *Constitution emergency and terrorism*, 2016, Naples, 7 ff.

De Stefani F., *The rules of Privacy. Practical guide to the new GDPR*, 2018, Hoepli, Milan.

De Vergottini G., *War and constitution: new conflicts and challenges to democracy*, 2004, Bologna, 209 ss.

Dorraji S. E*., Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations,* 2014, University of Oslo, Norway.

Dworkin R., *Terror and the Attack on Civil Liberties*, 2003 6 November, in The New York Review, 15-17.

Etzioni A., *How Patriotic is the Patriot Act? Freedom vs. Security in an Age of Terrorism*, New York, 2004.

Finn R. and Wright D., *Seven types of privacy*, 2013, Trilateral Research & Consulting, London
Michael Friedewald, Fraunhofer ISI, Karlsruhe.

Finn R., Wright D., and Friedewald B., *Seven types of Privacy,* 2013, in S. Gutwirth and others, European Data Protection: Coming of Age, Springer.

Gutwirth S., De Hert P., *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power*, 2006, Vrije Universiteit Brussel.

Hong Haeji, *Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao*, 2005, in Akron Law Review, Vol. 38 Issue 1, p71-111, 41p.

Hoofnagle C. J., *Federal Trade Commission Privacy Law and Policy*, 2016, Cambridge University Press.

Kobrin S. J., *Safe harbors are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance*, 2004, in Review of International studies, 30, 11-131.

Konvitz, M. R.: *Privacy and the Law: A Philosophical Prelude. Law and Contemporary*.

Lambo L., *The discipline on the treatment of the personal data: exegetical and comparative profiles of the definitions,* 2019, pg. 75.
Lodge F. Z., *Damages under the Privacy Act of 1974: Compensation and deterrence*,1984, in Fordham Law Review, Vol. 52, p611-636, 26p.

Long W. J., Quek M. P., *Personal data privacy protection in an age of globalization: the UE-EU safe harbor compromise*, 2002, in Journal of European Public Policy: 325-344.

Lukács A., *What is Privacy? The history and Definition of Privacy*, 2016, University of Szeged, Faculty of Law and Political Sciences, Department of Labor Law and Social Security and Sorbonne Law School Université Paris.

Markou C., *The Right To Be Forgotten. Ten Reasons Why It Should Be Forgotten*, ibid, pp. 203-226.

Marques J. F. M., *And they Built a Crooked Harbor – The Schrems Ruling and What it Means for the Future of Data Transfers Between the EU and US*, 2016, in EU Law Journal, p. 54 et seq.

Mordini E., *Whole Body Imaging at airport checkpoints: the ethical and political context*, 2011, Luxembourg.

Neil M. R., J. Solove, 2010, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev., 1887.

Nissenbaum H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, 2010, Stanford CA, Stanford University Press.

Pagallo U., *The protection of Privacy in the United States of America and Europe*, Milan, 2008, pp. 64-65.

Pagallo U., *La Tutela della Privacy negli Stati Uniti d'America e in Europa: Modelli giuridici a confronto*, 2008, Giuffrè Editore, S.p.A., Milano

Pagliaro P. S., *Delitti contro il patrimonio,*2003, Milan.

Park Taylor J., *Event Horizon: The Constitution approaches Guantanamo: A legal guide to the U.S. Detainee Cases*, 2004,in The Montana Lawyer, n.8, 512-569.

Pascuzzi G., *The law of the digital era*, 2010, Il Mulino, Bologna.

Pizzetti F., *Il percorso del Consiglio d'Europa che porta al riconoscimento del diritto alla Protection of personal data*, 2010, LUISS Guido Carli, Roma.

Ratner M., *Moving Away from the Rule of Law: Military Tribunals, Executive Detentions and Torture*, 2003, in Cardozo Law Review, vol.24, n.2.

Rodotà S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, 2014, Roma-Bari, Laterza

Rosenberg C., *Detentions at Guantanamo Bay "grave mistake" lawmakers*, 2003, Miami.

S. Rodotà, Introduction, in D. Lyon, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, 2002, Milano, page. XI.
Samuel D. Warren S. D., Brandeis L. D., *The Right to Privacy*, 1860, Harvard Law Review, Vol.4, No.4.

Saurugger S., Terpan F., *The Court of Justice of the European Union and the Politics of Law*, 2015, cit., pp. 158-179.

Scarborough A. S., *Nevada needs a Privacy Act: how Nevadans are particularly at risk for identity theft*, 2007, in Nevada Law Journal, Vol. 7 Issue 2, p640-663, 24p.

Slevin V. P., *Lardner G., Bush Plan for Terrorism Trials Defended*, 2001, in Washington Post, 36, cf. Cheeney.

Solove D. J., *The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure*, 2003 Duke Law Journal 967.

Sullivan J. M., *Will the Privacy Act of 1974 still hold up in 2004? How advancing technology has created a need for a change in the system of record saving*, 2003, in California Western Law Review 39 no2 395-412.

Tracol X., *Invalidator Strikes Back: The Harbor Has Never Been Safe*, 2016, in Computer Law & Security Review, p. 345 et seq.

Ustaran E., *The future of international data transfers*, 2018, Privacy & Data Protection Journal, Vol. 18, No 6.

Valvo A. L., *The right to be forgotten in the age of "digital" information*, in European Integration Studies, 2015, no. 2, pp. 347-358.

Westin A., *Privacy and freedom*, Atheneum, New York, 1970, p. 337.

Zangrilli O., *Open Government: dalla Semplificazione della P.A. alla e-Democracy*, 2018, LUISS Guido Carli, Roma.

Legislation and Soft Law

California Legislative information, AB-375 *Privacy: personal information: businesses.* (2017-2018) (2018-2019).

Commission Decision of 26 July 2000 *On the adequacy of the protection of personal data in Switzerland* pursuant to Directive 95/46/EC.

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council *on the adequacy of the protection*

provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

Convention No. 108, signed in Strasbourg on 28 January 1981, *On the privacy of persons with respect to the automated processing of personal data* signed on January 28, 1981 in Strasbourg.

Council of Europe Convention for the *Protection of Individuals with regard to the Automatic Processing of Personal Data* of 28 January 1981, n.108.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, *On the collection and protection of personal data in the electronic communications sector (EC) (Directive on privacy and electronic communications).*

Directive 2006/24/EC Of the European Parliament and of the Council of 15 March 2006, *On the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks* and amending Directive 2002/58/EC.

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

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997, *Concerning the processing of personal data and the protection of privacy in the telecommunications sector.*

Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted on 25 May 2018.

Law (EC) No 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on *the security of persons with regard to the collection and free movement of personal data by the institutions and bodies of the Community.*

Law no. 675 of December 31, 1996 , *Protection of persons and other subjects with regard to the processing of personal data,* entered into force in May 1997 *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.

Personal Data Protection Code, containing provisions to adapt the national legislation.

Presidential Military Order: *Detention, Treatment and Trial of Certain Non-citizens in the War Against Terrorism*, 66 Fed. Reg. 57, 833, 13 November 2001.

Regulation (EU) 2016/679 Of the European Parliament and the Council of 27 April 2016, *On the protection of individuals 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).

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

The EU/2016/679 General Data Protection Regulation (GDPR*): new rules EU and clarifications on personal data protection* Basic checklist for professional firms, Fondazione Nazionale dei Commercialisti, 2018.

The European Convention for the Protection of Human Rights and Fundamental Freedoms was signed in Rome on November 4, 1950.

The European Union's Charter of Fundamental Rights was declared in Nice on 7 December 2000.

The USA PATRIOT Act: *Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism),* 26 October 2001 to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

Case Law

Court of Justice of the European Union, Case C-13/94 of 30 April 1996, *P v. S and Cornwall County Council.*

Court of Justice of the European Union, Joined Cases C-468/10 and C-469/10, 24 November, 2011, *Asociación Nacional de Establecimientos Financieros de Credito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*

Court of Justice of the European Union joined cases C-293/12/C-594/12, judgment of 8 April 2014, *Digital Rights Ireland Ltd v. Minister for Communications*

Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.

European Court of Human Rights, case No.156/1996/976, 27 March 1998, *Petrovic v. Austria*

European Court of Human Rights, case No. 25576/04, 6 April 2010, *FLinkkila and Others v. Finland*

European Court of Human Rights, case No. 32265/10, 5 December 2013, *Henry Kismoun v. France*

European Court of Human Rights, case No. 10280/12, 3 June 2014, *López Guió v. Slovakia*

European Court of Human Rights, case No. 12738/10, 3 October 2014, *Jeunesse v. Netherlands*

Italian Court of Cassation, case No. 4487, 22 December 1956, *Associated production company Tirrena Asso film v. Caruso*

Supreme Court of the United States of America, case No. 5 U.S. 137, 1803, *Marbury v. Madison*

Supreme Court of the United States of America, case No. 381 U.S. 479, No. 496, 29 March 1965, *Griswold Et Al. v. Connecticut*

Supreme Court of the United States of America, case No. 389 U.S. 347, No. 35, 18 December 1967, *Katz v. United States*

Supreme Court of the United States of America, case No. 388 U.S. 1, No. 395, 12 June 1967, *Loving v. Virginia*

Supreme Court of the United States of America, case No. 405 U.S. 438, No. 70-17, 18 November 1971, *Eisenstadt, Sheriff v. Baird*

Supreme Court of the United States of America, case No. 75-89, 22 February 1977, *New York v. Roe Bt Al.*

Supreme Court of the United States of America, case No. 02-102, 26 June 2003, *Lawrence Et Al. v. Texas*

Sitology

http://gnosis.aisi.gov.it/gnosis/Rivista8.nsf/ServNavig/28

https://www.agendadigitale.eu/sicurezza/privacy/privacy-e-protezione-dati-personali-cosa-sono-quali-differenze-cosa-e-cambiato-col-gdpr/

https://www.jstor.org/stable/4540882?seq=1

https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

https://www.dirittocomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/

https://en.wikipedia.org/wiki/Right_to_privacy

https://www.carmillaonline.com/2003/07/23/faulkner-privacy/

http://www.privacy.it/archivio/rodo20051028.html

https://www.assiteca.it/2019/08/privacy-cose-il-diritto-alla-privacy-e-perche-e-bene-tutelarlo/

https://www.assiteca.it/2019/08/privacy-cose-il-diritto-alla-privacy-e-perche-e-bene-tutelarlo/#:~:text=8%20recita%3A,carattere%20personale%20che%20lo%20riguardano.&text=Tali%20dati%20devono%20essere%20trattati,fondamento%20legittimo%20previsto%20dalla%20legge.

https://it.wikipedia.org/wiki/Codice_in_materia_di_protezione_dei_dati_personali#:~:text=Il%20codice%20per%20la%20protezione,vigore%20dal%201%C2%BA%20gennaio%202004.

https://www.mruni.eu/upload/iblock/b97/ST-14-4-2-05.pdf

https://www.filodiritto.com/privacy-e-nuove-tecnologie-problemi-e-soluzioni

https://www.comparethecloud.net/articles/the-differences-between-eu-and-us-data-laws/

https://www.commerce.senate.gov/2020/12/the-invalidation-of-the-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows

https://www.kudos-data.com/eu-versus-us-privacy-legislation/

https://fas.org/sgp/crs/row/IF10896.pdf

https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/how-do-eu-and-us-privacy-regimes-compare

https://www.compliancejunction.com/differences-european-privacy-laws-american-privacy-laws/

http://www.adir.unifi.it/rivista/2005/surace/cap2.htm#n59

https://www.agensir.it/quotidiano/2000/5/3/privacy-rodota-uomini-di-vetro-in-una-societa-trasparente/

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1744986

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1335256

https://www.agensir.it/quotidiano/2020/6/23/privacy-soro-garante-protezione-dei-dati-e-uno-straordinario-presupposto-di-democrazia/

http://www.rogerclarke.com/DV/

http://www.rogerclarke.com/DV/Intro.html

https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection-explanatory-memo

https://www.privacylab.it/IT/989/come-si-e-arrivati-al-gdpr-dalla-privacy-al-regolamento/

https://www.cortecostituzionale.it/actionSchedaPronuncia.do?param_ecli=ECLI:IT:COST:1973:38

Executive Summary

The issue of personal data is one that has become increasingly important in recent years, particularly due to the rapid growth of the Information Technology sector and Communication platforms.. If, on the one hand, globalization, technological evolution and freedom of communication have been drivers of secure growth and planetary economic trade over time, on the other hand, individual privacy protection problems have arisen and, more recently, problems of security and national public order.

The right to privacy is consistent with the *"right to be left alone"* in the United States. The latter, discovered in the 1890 publication of the essay The Right to Privacy, signed by Samuel D. Warren and Louis D. Brandeis, contributed to the development of the principle of security with the attribution to the individual of the right to be left alone, undisturbed, to enjoy, thereby, a private domain safe from the intrusion of outsiders.
For a long time, this U.S. principle of privacy, characterized by a strict jurisprudential nature, found ground in the European legal landscape before technologically advanced society imposed a strong need for redefinition.

In Europe after the historical experience of the mass abuse of personal data by authoritarian regimes, in particular by sensitive ideological and political affiliation data, the institutional manipulation of the repressive and anti-democratic key has all been misused. The need for individual protection against interference in privacy was necessary in order to gain importance as a constitutionally protected right and, as such, to be protected not only against individuals but also against public power. The history of the Council of Europe and the jurisprudence of the European Court of Human Rights have contributed to this European idea of the right to privacy.
The right to the privacy of personal data was established in such a way that the provisions of Directive 95/46/EC were initially applied and eventually implemented in a jurisprudential manner.

Finally, the same was legally “consecrated” within the framework of the ad hoc clause laid down in Article 8 of the Charter of Fundamental Rights of the European Union, which was granted binding force by the Treaty of Lisbon, taking it to the same level as other treaties.
This recognition thus distinguishes European law from the legal traditions of other Western democracies, such as, in particular, the United States of America, and is also an explanation of its particular significance in the sense of legislative security.

Whereas, in Europe, the protection of personal data specifies the objects of the protection sought by an instrument of general law in the general and universal legal framework, in the United States, on the other hand, the Federal Constitution does not apply explicitly to the protection of personal data in the list of constitutional rights.
The latter is drawn up on the basis of highly sectoral and decentralized legislation, specifically distinguishing between the private and public sectors where the framework for self-regulation is in effect. In addition, the current challenges posed by technological development to Europe relate to the defense of the private sphere from the modes of regulation that modern technology can exercise, through the arrangement to unique regulatory remedies. Thus, we have advanced from the initial right to privacy to data protection after a long evolutionary period, which has deteriorated as a fundamental citizen's right under both the national and EU legal systems.

As such, the right to the privacy of personal data protects an individual's data, interpreted as a compilation of information relating to different aspects of the life of a person (both his or her private sphere and his or her social sphere) that the person concerned wants to make available to the public or, on the contrary, decides not to disseminate.

In addition, the paradigm of privacy and the concept of personal data protection itself has evolved over time: it has moved from an original, purely

“content” definition of data protection to a more data protection-oriented view, relating to the regulation and protection of the right to property, to a decline in the rights of freedom and dignity of the individual. The importance of dominating our information properties, along with a greater knowledge of the use of our personal data in a 'digital society' in an age such as today, in which the use and sharing of information for various purposes has reached its historical peak and is destined to escalate exponentially, are necessary elements in order to preserve the fundamental core of personal freedoms.
The right to the protection of personal data is therefore a legitimate protection of all fundamental rights in a digital world and in electronic communications technology.

Notwithstanding, in recent years, there has been another factor which has strongly affected this issue: terrorism. Following the September 11, 2001 attacks in the United States, the course taken was toward greater control at the expense of privacy and the protection of personal data. The European Union (EU) has favored safeguarding the protection of personal data, by contrast.
At present, there is no internationally agreed regulation on the protection of personal data. Part of the challenge of reaching an agreement is that it is a morally contentious environment in which the right of speech or national protection against privacy has been continuously resisted.

At this juncture, both the European Union and the United States are aware of the importance of this issue and tend to be involved in ensuring adequate data protection measures to sustain their secure ties, both economically and in terms of national security and protection for their people. Therefore, it is important to take account of the regulatory structure, which tends to be fragmentary and heterogeneous but which, at the same time, is the protagonist of multiple legislative initiatives introduced to achieve a more organic supervisory system.
Therefore, as a natural and inevitable consequence of international commercial transactions and of the interconnectedness of interpersonal relations in the

internet age, the current General Regulation on the protection of data outside the territories of the Union is not a secondary function.

The principles governing the lawfulness of transfers of personal data to third countries under European law have already been established in this specific matter and the regulatory frameworks applicable to the European Union in this field have been examined.

All this with the objective of ensuring an adequate level of security for the transfer of personal data, which today appears to be one of the real foreign policies of the European Union, with the objective of ensuring a high level of protection of the data of European citizens, irrespective of their place of residence, within the meaning of international relations with third countries.

The aim of the Privacy Shield Agreement was to ensure the protection of European citizens' data in the event of data transmission to servers located in the American territory, which replaced the previous Safe Harbor Agreement after the censorship pronouncement of the European Court of Justice. With the imposition of stricter obligations, attempts have been made to provide stronger protection for American companies processing data from European citizens by means of a very stringent control and monitoring system placed in place by the European Union authorities.

In this new context, the object of the Right to be Forgotten is to ensure that the individual has complete control over his own knowledge. In the judgments articulated at European and American level, the possibility that the Institute of the Right to be Forgotten gives the involved party the power to delete signs of its own past, potentially weakening the exercise of the right to know, has created numerous contrasts.

In conclusion, it should be recalled that, considering the undoubted progress made by the elaboration of the Right to be Forgotten by the Institute, the prospect of being able to neutralize a piece of news in the digital *galaxy* in an absolute manner remains quite difficult at present.

This work will explore the recent development of the Personal Data Protection Act, both in the European panorama and in the United States, and its relationship with the most important realities surrounding it, showing the lights and shadows encountered thus far by lawmakers, as well as analyzing the parallels with other realities around the world.

The first chapter will offer a historical overview of the birth and evolution of personal data security.
Starting from the common core of the Right to Privacy, primarily understood as the right to be left alone, it will come to the experience of the oppressive states of the early '900, expanded in the popular article by Warren and Brandeis in 1890, which will dramatically shift the understanding of the two increasingly different definitions of Privacy and Personal Data Protection.

In the second chapter, the key legislative instruments introduced over the years in the field of privacy and the protection of personal data in the European system will be analyzed. Initially, the Community legal system, formulated from an economic integration point of view, did not consider the question of privacy regulation by clear legal provisions. However, Europe has also taken steps to protect, through the jurisprudence of the courts, the fundamental values of the citizen. In the evolutionary process and in the ensuing legal recognition of the right to privacy as an independent condition worthy of protection on our continent, there have also been some complexities.
The importance of the principles enshrined in Directive 95/46/EC, which have long been the basic source of protection of personal data, will be examined. Finally, the Italian data protection experience, along with the most relevant reference to privacy, which can be found in Article 2 of the Constitution, which deals with privacy in terms of the inviolable rights of human beings, will also be analyzed.

The third chapter will focus entirely on the study of the legislative structure of the United States. At the end of the nineteenth century, the principle

of privacy was born in the United States to guarantee the protection of ideas and feelings as an extension of the right to private property against the growing intrusiveness of printed paper. However, the protection of privacy in the federal law of the United States of America is very ambiguous and there is, for the same reason, no specific legal meaning in the federal system. This is due to the fact that several different legal circumstances are involved in its definition.
Without any doubt, the US law on the security of personal data provides a more fragmented regulatory framework. At a fundamental level, the Fourth Amendment to the Constitution protects privacy and personal data.

The fourth chapter will concentrate on the study of the transfer of personal data to third countries and, in particular, the problems that have arisen in this regard with the United States. It seeks to investigate the developments that have affected the international regulatory scenario in the light of the revelations of Edward Snowden about the US intelligence programs, which, in turn, have created a mechanism capable of subverting the dynamics related to the transfer and transformation of personal data, even due to the lawsuit of Maximilian Schrems against the social network of Facebook.
The Privacy Shield Agreement, which entered into force on 12 July 2016 and expired with Case Schrems II in 2020, will be discussed and the identification of its key points and characteristics that differentiate it from the previous Safe Harbor Agreement will be illustrated.

Finally, in the fifth chapter, I will treat the *Right to be Forgotten* in a comparative context. It will determine in this context whether a general and theoretical ideal concept of the *Right to be Forgotten* can be established that would go beyond jurisdiction. The analysis will focus on the two major jurisdictions, the EU and the US, clarify the EU-described meaning, and then question the current narrative that the right to be forgotten is not consistent with the US.
It focuses on the evaluation of the effects on the definition of the word of the case of CJEU Google Spain-Costeja, including on the study of EU and US case

law. The CJEU has adopted a groundbreaking decision in the history of data protection. By officially acknowledging the existence of the right to be forgotten in the legislative sense of the EU, it clarified the role that the EU market can play in relation to personal data and privacy, the effects of which are crucial for the evolution of the privacy rules.
Moreover, the U.S. constitutional and ideological framework is compatible with the manner in which the EU has treated the essence of the *Right to be Forgotten*. Consequently, the transition to a more privacy-friendly legal structure, ready to accept the right to be forgotten, could be viable if such technical and institutional barriers are overcome.

One aspect is visible, however. In the absence of a consistent approach to life and law enforcement, the inconsistencies in the vision between the US and the EU cultures will escalate, leading both to the intensification of current issues and to the emergence of new ones. In addition to being inconsistent from one jurisdiction to another, law enforcement may transform legislation into a field of unpredictability and misunderstanding. This would contribute to unjustified inequalities in the care of individuals and private institutions, which would weaken the justice system's overall trust. The economy would also be impacted in order to comply with the discrepancies, since companies will be forced to take undesired measurements.