LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department: LAW

Teaching: PUBLIC COMPARATIVE LAW

BOUNDARIES BETWEEN *INDIVIDUAL PRIVACY* AND *NATIONAL SECURITY*: A COMPARATIVE STUDY

SUPERVISOR

Prof. Andrea De Petris

CO-SUPERVISOR

Prof. Gino Scaccia

CANDIDATE

Alessandro De Giacomo

STUDENT N. 103593

Academic Year 2013-2014

To my Parents
Grazia and Giuseppe,
and to my Brother Carlo
for their constant support
and unconditioned love.

“They who can give up essential liberty
to obtain a little temporary safety
deserve neither liberty nor safety”.
Benjamin Franklin

Contents

Chapter III

The *Datagate Scandal*: *Individual Privacy* vs. *National Security*

Introduction

June 2013 was a crucial month for the realization of this *Thesis*. In fact, at the beginning of the month, I found out I was going to participate in the *Advanse AMERIGO*, a *LUISS University*-sponsored *American* internship program, based in *Washington D.C.* At the time, in fact, I was completing my fourth year of law school, and was already thinking of the subject for my final dissertation thesis, in 2014. Further more I had decided to focus my research in the *Public Comparative Law* field, after taking the course exam in May.

A few days later, however, I also discovered from *The Guardian* newspaper about the *Datagate Scandal*. I was shocked from how the *American Government* had apparently breached, what I believed to be internationally recognized, *Individual privacy* standards, in the name of *National security*, through the surveillance programs of its *National Security Agency (NSA)*. The coincidence was almost astonishing; therefore, I decided I would take advantage of my presence in the *U.S. Capital*, to investigate further on the matter.

In fact, I have always been fascinated by the *right to privacy*, and by its evolution over time, being part of the "big brother-generation", where everything we say and do is somehow registered. At the same time, though, I was very interested in *National security* standards, especially since the *9/11 Attack*, during which I studied in one of the few *American* schools of *Rome*, deeply affected and literally transformed in an *U.S. Embassy*-like protected bunker, since the *Attack*.

On one hand, I was thrilled at the idea I could "spy on the spies", yet, on the other hand, I was quite scared my *VISA* would be revoked, or that I would spend the rest of my days in *Guantanamo*, for minding the *American Government*'s business. This, however, was another consequence of being

part of my generation, nourished with *Hollywood*'s schemes and intrigues. However the *Scandal* had definitely not contributed to believe that movies like *Tony Scott*'s "Enemy of the State" (1998) were fiction.

Further more, in November 2013, on the first day I entered the *Library of Congress*, a librarian did actually admonish me, to avoid surfing websites as *Wikileaks*. She told me that all the Federal employees, including herself of course, had been given the same advice, and not as nicely, immediately after the previous *Wikileaks Scandal*. My probably ridiculous fears of getting expelled from the *U.S*. Territory were rising again. However, the librarian also gently advised me to consult the *American Civil Liberties Union (ACLU)*, "the watchdog of the *Nation*'s rights", in order to find out more about *Datagate*. Definitely a greater amount of information than the little I found later, in the law section of the *Library of Congress*.

No matter if inspired by the recent *Scandal*, and by curiosity of course, though, my idea was to review the entire history of *privacy* laws, in the *U.S.* and in the *EU*, and their *security*-related limits, and *boundaries*. Only then, was I going to analyze *Edward Snowden*'s revelations, and the consequences it provoked in the *United States* and in the *European Union*.

In fact, in order to understand and compare the current *privacy-security* standards, on both sides of the *Atlantic Ocean*, I had to review the *U.S.* legislation on the matter, first, and the *EU*'s, afterwards.

Further more, as a citizen of an individual *EU Member State*, specifically of *Italy*, a Civil law-legal order with its own *Constitution*, I had always traced to the latter the origins and the legality of any right, legal principle, or provision, including *privacy*'s, of course. However, the analysis and comparison between the *privacy-security* relation of the Common law-legal order of the *United States*, a *Federation* of 50 (almost entirely) Common

law-regulated *States*, and the *European Union*, a *Union* of currently 28 sovereign *National States*, with different legal traditions, had to necessarily take into account the common constitutional traditions, but also the ordinary laws, the jurisprudence, and the International Treaties and Conventions, regarding all the parties involved.

Therefore, taking into account the evolution of *U.S.* privacy law, from *Warren*'s and *Brandeis*' "right to privacy" to the latest *Emergency Legislation* (*Patriot Act*, *PRISM*, etc.), the evolution of *EU* privacy law, from the *Convention for the Protection of Human Rights and Fundamental Freedoms* to the *Data Protection Directives* (*Directive 95/46/EC*, *Directive 2009/136/EC*, etc.), and given *Datagate* and its consequences, the *boundaries* between *Individual privacy* and *National security* will result uncertain.

However, while *National security* "always" prevails in the *United States*, because of their recent history and of their missing strong Federal *privacy* protection, the *European Union*, instead, has a major focus on *Individuals*, and their private rights, especially given its *Member States*' strong *Individual*-based common constitutional traditions.

Finally, I will point out, that beyond the limited, but hopefully progressive, *Governments*' *privacy* policies, both in the *U.S.* and in the *EU*, it is up to us citizens, in the end, to protect our *privacy*, learning about our rights, and taking careful action, especially on the web, definitely the greatest technological innovation of our time, but also the greatest threat to our *privacy* and *security*.

Chapter I

Individual Privacy and *National Security*

In the *United States*

1. The *Right to Privacy*

In the *United States privacy* laws comprehend different legal concepts. For example, *privacy* can refer to the *invasion of privacy*, "a tort based in Common law allowing an aggrieved party to bring a lawsuit against an individual who unlawfully intrudes into his or her private affairs, discloses his or her private information, publicizes him or her in a false light, or appropriates his or her name for personal gain." [1] However, to fully understand these legal concepts, we should review the historic evolution of *privacy* in the *United States*.

The most important legal concept in *U.S. privacy* laws is the *right to privacy*, first defined, in 1890 by *Samuel Warren* and *Louis Brandeis*, as "the right to be let alone."[2] At the time, in fact, the two famous *Boston* lawyers published an article entitled "The Right to *Privacy*", in which they explained why they believed it was necessary to introduce a new right in the *North American* legal system. This small masterpiece, less than thirty pages long, described *privacy* as a fundamental individual right, which therefore enabled private citizens to bring a lawsuit in front of an impartial and independent judge.

---

[1] "Invasion of Privacy Law & Legal Definition", *US Legal*, (*www.uslegal.com*).
[2] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 195.

In the article's introduction, the *Authors* explained why they wrote it: "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society".[3] In the same article, *Warren* and *Brandeis* also shifted their focus on newspapers: "The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers...The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and *privacy* have become more essential to the individual; but modern enterprise and invention have, through invasions upon his *privacy*, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[4]

Further more, *Warren* and *Brandeis* clarified their goals: "It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the *privacy* of the individual; and, if it does, what the nature and extent of such protection is".[5] Keeping in mind the nature of the *American* judicial order, based on the *stare decisis* principle, the *Authors* could base their theories only on a few precedents: beyond the quotes of Justice *Thomas F. Cooley*, they mentioned the case of *Prince Albert*

---

[3] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 193.
[4] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 196.
[5] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 197.

against *Strange*, the one of *Abernethy* against *Hutchinson*, and a few others.[6] However, the greatest dilemma at the time was how to defend the theory of jurisprudence as a source of law in a system that was inspired, at the same time, by the *stare decisis* principle? *Warren* and *Brandeis* handled this issue with a brilliant solution, specifically with "the elasticity of our law, its adaptability to new conditions, the capacity for growth, which has enabled it to meet the wants of an ever changing society and to apply immediate relief for every recognized wrong, have been its greatest boast".[7]

Finally, the *Authors*, recognizing that technological advances would become gradually more relevant, stated: "Now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation".[8] Their theory was that, initially, the law "offered only remedies against physical interference and violent acts of transgression in the lives and property of individuals". But from then onwards also the spiritual nature of men was to be recognized, adding safeguards to protect people's reputation against defamatory statements, and other intangible rights, such as those arising from the intellect.[9] In fact, "the beautiful capacity for growth, which characterizes the Common law, enabled the Judges to afford the requisite protection, without the interposition of the legislature".[10]

---

[6] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 207.
[7] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 213.
[8] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 211.
[9] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 213.
[10] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 195.

For this reason, while in 1902, the *District Judges* in *New York* still rejected the demands of a young woman who, without her consent, found herself "lithographed" on about 25 thousand leaflets of the *Franklin Mills Flour*, with the slogan "Flour of the Family," it is significant that, later on, the *State of New York* took remedy for it with a special Statute, approved in 1903.[11] Further more, two years later, the *Court of Georgia* recognized the institution among the cases of civil liability provided by *common law*.[12] In the evolution of the legal system a new right was born: *The Right to Privacy*[13].

After the *Warren* and *Brandeis*' article, there have been at least three hundred different cases concerning a breach of *privacy,* in terms of civil liability. In fact, in the early years of the twentieth century, even the *Supreme Court of Washington* handled more often cases of the kind. For instance, the *right to privacy* was recalled in 1905 already, in the case *Lochner v. New York*, regarding contractual choices of the parties in labor relations[14]. The *right to privacy* was also invoked in the *Meyer v. Nebraska* case (1923), in regards to the right to learn and to the use of foreign languages[15], and in the case *Pierce v. Society of Sisters* (1925), on the choice of schools (including non-governmental ones)[16].

Further more, this theory of the "beautiful capacity for growth"[17] that characterizes the *North American* Common law, offered by *Brandeis* and *Warren*, was then emphasized by *Carleton Kemp Allen* in 1927, in his "Law in

---

[11] *N.Y. Civ. Rights Law §§ 50-51.*
[12] *Pavesich v. New England Life Insurance CO.*, 50 S.E. 68, Ga. 1905.
[13] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, pages 193 - 220.
[14] *Lochner v. New York,* 198 U.S. 405, 1905*: precedent was later abandoned.*
[15] *Meyer v. Nebraska,* 262 U.S. 390, 1923.
[16] *Pierce v. Society of Sisters,* 268 U.S. 510, 1925.
[17] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 195.

the Making".[18] This expression had a double meaning. On one hand, as opposed to "Law in the Books", it suggested an alternative approach to the typical formalism of continental Civil law, where the law coincided with what is expressly stated by the Legislator[19]. On the other hand, the expression "Law in the Making" focused on the way the law actually evolves and develops over time [20]. However, *American privacy* policy must be fundamentally divided into two parts. The first concerns a set of principles, provisions and amendments to the *Constitution*, as interpreted over the centuries by the *Supreme Court* in *Washington*. The second concerns the ordinary law, both at the level of *Statutes* and of Common law.

2. Prosser's Four *Privacy* Torts

In 1960, *William Prosser* published an article regarding privacy on the *California Law Review*[21]. *Prosser*'s publications obtained almost the same success as that achieved by the one of *Warren* and *Brandeis*, seventy years earlier. Therefore, according to the scheme, already seen at the beginning of the century, a simple article published on a law review, resulted in influencing the work of the *Courts*, denoting once again the particular influence of doctrine over jurisprudence, which started fully implementing *Prosser*'s view[22], and setting aside the one established by Judge *Brandeis*[23].

---

[18] Allen C. K. - *Law in the Making*, Third edition. M.C., M.A., D.C.L. Oxford: Clarendon Press. 1939.
[19] Pagallo U. and Gentile F. - *Testi e contesti dell'ordinamento giuridico: Cinque studi di teoria generale del diritto*, Padova, CEDAM, 1998, page 61.
[20] Abernathy F. – *Defining "Privacy": The Power of Culture in a Digital Age,* in Privacy: Altre Voci (Ugo Pagallo ed., 2005), page 4.
[21] Prosser W. L. – "Privacy, a legal analysis", *California Law Review*, n.48, 1960, pages 383-423.
[22] Blounstein E. J., for example, reported more than 15 cases in the area of privacy that had already applied Prosser's theoretical setting ("Privacy as an aspect of human dignity: an answer to Dean Prosser", *New York University Law Review*, 1964, page 964, footnote 10).
[23] Wade D. describes the influence of Prosser' Article: "Another event that could quickly bring the level of the law to his maturity took place about four years ago, and could even change the habit of

In fact, during a study of tort law, *William Prosser* stated that the *right to privacy* encompassed four types of lesions, of four different interests of the person: "One who invades the right of *privacy* of another subject to liability for the Resulting harm to the interest of the other. The *right of privacy* is invaded by (a) unreasonable intrusion upon the seclusion of another...; or (b) appropriation of the other's name or likeness...; or (c) unreasonable publicity Given to the other's private life...; or (d) That publicity unreasonably places the other in a false light before the public..." (*Section 625A*)[24].

Further more, *Prosser* identified four specific figures of privacy, after analyzing more than three hundred selected cases, thus calling into question various interests[25]. These figures were taken under the same name, but their characteristics were very different. He described an interest in being free from "mental distress", in the first case, an owner's interest, in the second case, and an interest in reputation, in the third and fourth cases. The only thing in common between the different figures was to represent each undue interference with the right of the plaintiff, which he identified once again as a "right to be let alone", in reference to the, already mentioned, expression of Judge *Thomas Cooley*.

Beyond this, the *Author* focused on the behavior of the defendant and on the interest to be protected. These were the criteria that lead him to identify the four figures, in the name of an interpretative tradition of Tort Law[26]. *Prosser* argued that his theory was able to bring order to what Judge

---

referring to the article by Warren and Brandeis; it is seen as the origin of the nature of the right (to privacy), as well as its true description" (*Virginia Law Weekly Dicta*, October 8, 1964, p. 1, col. 1).

[24] Prosser W.L. and Wade J. W. - "Restatement of the Law, Second, Torts", *American Law Institute*, 1961, *Section 625A*.

[25] Prosser W. L. – "Privacy, a legal analysis", *California Law Review*, n.48, 1960, page 388.

[26] In the common law legal system the term "tort" can be understood as a first approximation of the tort of our civil law legal systems, but in common law the term has a broader scope and includes

Biggs had defined as "a pile of hay in a hurricane", in 1956[27]. The disorder of jurisprudence, in his opinion, was due to the inability to separate and distinguish these four types of *privacy* breaches, which required a different treatment by the legal system. The order desired by *Prosser* was found, but definitely in negative terms, for those who believe that *privacy* represents a value to be protected in an extensive way.

In fact, the crystallization of the four figures of the *privacy* Tort, which substantially bring us back to a system of *writs*[28], has led to a strong compression of the *right to privacy* in Tort law, and in all its manifestations. Therefore, the thus configured law, whenever in competition with other constitutionally guaranteed rights, such as the “freedom of the press”, could only succumb.

The picture of the success of these figures in the *American Courts* is not promising. Actually, not all are recognized in several *States*: the more refractory is *Minnesota*, which denies accepting all four of *Prosser*'s Torts. However, when they are recognized, the affixing of terms and conditions, reduce their practical impact. Moreover, the fragmentary nature, and the crystallization of these Torts, stratified by time and by case law, are not able to act as a bulwark of privacy, especially when it comes to balancing the latter with other interests of constitutional significance. Considering the needs of modern times, and the pressures that come from other legal cultures, further doubts arise, on the fact that these Torts are not, yet, in the

---

other legal situations, ranging from the contract, and / or the rights of the person, and / or real rights in general (Markesinis B.S. and Deakin S.F. - *Tort Law*, 4th Edition, Clarendon Press, 1999).

[27] *Ettore vs. Philco Television Broadcasting Co*., 229 F.2d 481 (3rd Cir. 1956).

[28] In common law the writ was the tool that allowed the technical functioning of justice implemented by the English monarchs. It was necessary in order to have a protection of the law: an individual right could be said to exist in as much as there is a writ that would make it operable. Hence the statement that "remedies to prior rights", which corresponds to the Roman law "remedium ubi, ibi ius".

position to provide the necessary tools for the protection of *privacy*. It is, therefore, necessary to look at other routes and other instruments.

3. U.S. Constitutional *Privacy* Law

No matter if the *Court* declared, in the case *Katz. v. United States* (1967), that "the protection of the general *right to privacy* due to individuals depends largely on the law of individual *States*"[29], there are at least two reasons to start our analysis from the *privacy* protection granted by Constitutional law at a Federal level. First of all, the *American* legal system provides the Constitutional control of ordinary *State* laws. Secondly, the Constitutional protection in the *United States* prohibits the *Federal Government*'s intervention in individuals' personal affairs. It is up to each *State*, instead, to ensure a greater amount of *privacy* protection, through positive legislation, than the minimum required Constitutionally.

On the basis of these premises, we shall examine the Constitutional system of *privacy* at the Federal level first, distinguishing a public sphere from a more private one. Later on, we will focus our attention on the major consequences, in terms of *privacy* law, produced by the most recent technological innovations.

4. The Public Sphere of Constitutional *Privacy*

Regarding the public sphere of Constitutional *privacy*, it is necessary to further distinguish the right to *privacy* between "the right to perform political activities anonymously", and "the expectation of *privacy* in public places". Regarding the private sphere of Constitutional *privacy*, instead, the distinction to be made is between the rights "to procreation", "to intimacy"

[29] *Katz. v. United States,* 389 U.S. 347, 1967.

and of course “to a sexual sphere”. The Constitutional protection of anonymous political action derives from the provisions of the *First Amendment* to the *Constitution*, particularly in regards to *freedom of expression* and to *freedom of association*: “*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.”[30]

On the matter, an emblematic case is the one occurred during the civil wars of the fifties, between the *National Association for the Advancement of Colored People (NAACP)* and the *State of Alabama*. In fact, in front of the latter's request to get hold of the list of members of the *NAACP*, the *Court* recognized the "vital relationship" between *privacy* and *freedom of association*, and that "the inviolability of *privacy* may result in many circumstances necessary to preserve the freedom of association, especially when a group adheres to dissenting opinions", therefore denied *Alabama*’s request.[31] Only two years later, in 1960, there was a similar issue, in the case *Talley v. California*, in which the *Court* declared the *State* law, that prohibited the distribution of anonymous leaflets, “unconstitutional”. The reason of this decision was not only to prevent sanctions or retaliation by public authorities, but also by any citizen who could eventually come into possession of the same information.[32] By the way, this approach was confirmed in the fairly recent case *McIntyre v. Ohio Board of Elections,* in 1995: "The interest for anonymous works to enter the marketplace of ideas

[30] “First Amendment”, *U.S. Constitution*.
[31] *NAACP v. Alabama*, 357 U.S. 449, 1958.
[32] *Talley v. California,* 362 U.S. 60, 1960.

has undoubtedly greater importance of each public interest in requiring disclosure of names. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of the publication, is an aspect of the *freedom of speech*, protected by the *First Amendment*".[33]

Further more, the technological revolution has not changed much in terms of *freedom of speech*. In fact, once more, in its 2002 ruling on the case *Watchower Bible & Tract Society of New York v. The Village of Stratton*, the *Court* declared the legislation, that required prior registration with the *Government* of individuals who promoted their ideas from door to door, "unconstitutional", considering it in contrast with the *First Amendment*, and with the *right to anonymity*.[34]

The second type of cases relating to *privacy* in a public place, calls into question the protection provided by the *Fourth Amendment* against unreasonable search or seizure: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".[35] An important example is the case *Katz v. United States*, which concerned the proceeding brought by the *Federal Government* against a bookmaker that was placing bets unlawfully, by means of a public telephone. The *Court* ruled: "as an individual in the office, in a friend's apartment or in a cab, a person who is in a telephone booth may rely on the protection of the *Fourth*

[33] *McIntyre v. Ohio Board of Elections,* 514 U.S. 334, 1995.
[34] *Watchower Bible & Tract Society of New York v. The Village of Stratton,* 122 S. Ct. 2080, 2002.
[35] "Fourth Amendment", *U.S. Constitution*.

Amendment. One who occupies the cabin, closes the door behind him, and pays a token that allows him to make the call, is certainly entitled to believe that the words said during the call will not be circulated in the World. Reading in a narrower sense the *Constitution* means ignoring the vital role that the public telephone has come to have in private communications".[36]

Of course, the right to *privacy* encounters its limits in the "reasonableness" of the Constitutional Acts of the *Federal Government*, in order to ensure *National security*. In fact, the *Katz* case doesn't allow a terrorist to plea the *Fourth Amendment*, in order to organize undisturbed a terroristic attack, but on the matter we will see specific legislation (*Patriot Act*, above all), further on. Never the less, the importance of this case depends mainly on the fact that *Justices* of the *Court* have recognized, for the first time, that the guarantees on *privacy* conceded by the *Fourth Amendment*, are valid independently of the public or private nature of places (a public telephone booth, in this case). In other words, it has to be determined whether the individual interest for *privacy* prevails over the public's one, since "the *Fourth Amendment* protects people, not places."[37]

Therefore, technological innovations, urged on one hand the legislator to provide remedies, for example with the *Electronic Communications Privacy Act* in 1986, which authorized not only e-mails' interceptions, and turned-on phone numbers' registrations, but also those of the entire e-mails' content, and even the content of all media used by a specific person (in this case, however, an authorization by the Attorney General is requested).[38] On the

---

[36] *Katz v. United States,* 389 U.S. 347, 1967.
[37] Id.
[38] *Electronic Communications Privacy Act (ECPA)*, 18 U.S.C. § 2510-22, 1986.

other hand, these technological innovations made it harder to distinguish between private and public, or internal and external spaces.

A very particular case on the topic, occurred recently, is *Kyllo v. United States* (2001). In this case, in order to obtain a warrant, the Police used a thermal imaging device to prove a marijuana growing operation in *Kyllo*'s (the defendant) home, from outside the house. On the matter, the *Court* ruled "we believe that using sensory enhancement technologies to gather any information regarding the interior of the house, which could not otherwise be obtained without physical intrusion into a Constitutionally protected area...constitutes a search, at least when (as in this case) the technology used is not of general public use."[39] Of course this ruling makes it clear that technological development, especially if related to technology "of public use", may contribute to diminish Constitutional guarantees, in terms of *privacy*. But, of course, this process had started already with planes flying over people's houses; therefore, in 2001, the Court concluded "it would be foolish to assert that the degree of *privacy* guaranteed to citizens by the *Fourth Amendment* is immune from technological progress".[40]

5. The Private Sphere of Constitutional *Privacy*

Regarding private sphere of Constitutional *privacy*, instead, we already mentioned the distinction that occurs between the "right to procreation" and the "right to a sexual life" of each individual. The origin of this uncertain boundary between the two can definitely be found in the case *Griswold v. Connecticut* (1965), regarding a ban on the use of contraceptives, as an alternative to the *coitus interruptus*. At the time, the *Court* surely contributed

[39] *Kyllo v. United States,* 533 U.S. 27, 2001.
[40] Id.

to the so-called “sexual revolution”, stating the unconstitutionality of the ban, careless of the absence of an express Constitutional provision on the matter: "Perhaps we should allow the police to investigate into the sacred precincts of marital bedroom, looking for signs of the use of contraceptives? The very idea is repugnant to the notions of *privacy* surrounding the marital relationship."[41]

Other important cases at the Constitutional level of intimate privacy were *Roe v. Walde* (1973), which substantially recognized the Constitutional legitimacy of abortion[42], *Planned Parenthood of Central Missouri v. Danforth* (1976), which claimed that the father’s or husband’s consent was not necessary for abortion[43], and also *Bowers v. Hardwick* (1986), regarding the request from a gay couple of a Constitutional *privacy* protection to be granted to their intimacy[44]. While in the latter ruling the *Court* basically upheld the *State of Georgia*’s criminal prosecution of homosexual relationships, in the recent case *Lawrence v. Texas* (2003) the *Court* overruled *Bowers*. In fact, the majority agreed with Justice *Kennedy*: “"When sexuality is manifested clearly in the intimate conduct with another person, such behavior is nothing more than an element of the personal bond"[45], which is Constitutionally protected. No matter the dissenting opinions on the case, of Justice *Antonin Scalia* and two others, this landmark decision invalidated *sodomy law* in *Texas* and, by extension, in thirteen other States, making same-sex sexual activity legal in every *U.S.* State and Territory[46].

---

[41] *Griswold v. Connecticut*, 381 U.S. 479, 1965.
[42] *Roe v. Walde,* 410 U.S. 113, 1973.
[43] *Planned Parenthood of Central Missouri v. Danforth,* 428 U.S. 52, 1976.
[44] *Bowers v. Hardwick,* 478 U.S. 186, 1986.
[45] *Lawrence v. Texas,* 539 U.S. 558, 2003.
[46] Id.

The *Lawrence* ruling is based on the conception that a consensual sexual conduct is among the liberties provided by *substantive due process*, and specifically by the *First Section* of the *Fourteenth Amendment*: "All persons born or naturalized in the *United States*, and subject to the jurisdiction thereof, are citizens of the *United States* and of the *State* wherein they reside. No *State* shall make or enforce any law which shall abridge the privileges or immunities of citizens of the *United States*; nor shall any *State* deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."[47]

We can easily conclude that constitutional guarantees of *privacy* are often indirect, therefore not expressly among the *U.S. Constitution* articles, but found in *Amendments* (we referred already to the *First, Fourth* and *Fourteenth*) and, most of all, granted by the *Supreme Court*'s rulings. Let us now analyze, instead, ordinary *U.S.* legislation, in terms of *privacy*, both at a Federal and at the individual *States*' level.

6. Federal *Privacy* Law and the *Privacy Act*

Surely, the *Privacy Act*, approved by *Congress* on December 31st 1974, after the *Watergate* scandal regarding former *U.S.* President *Richard Nixon*[48], has been playing a pivotal role in terms of Federal *privacy* policy. This *Law* consists in one article, *n. 552 of Title V of the United States Code*, divided into twenty-one sections, filed in alphabetical order. The *Privacy Act*, or *Public Law § 93-579*, was conceived as an operational tool to strengthen the safeguards provided by the *Fourth Amendment*.

---

[47] "Fourteenth Amendment", *U.S. Constitution*.
[48] *Privacy* Act, Public Law 93-579, 88 Stat. 1897, in 5 U.S.C. n 552, 1974.

In fact, the *Law* states, in *paragraph (b)*, that no public institution can transmit to any person, or third party, data relating to an individual, without obtaining his prior consent or written request. Twelve exceptions are provided, though. Among these, are the cases that concern the use of statistical data storage, *Government* Agencies' routine acts, and investigations conducted by *Congress*, beyond law enforcement and specific administrative purposes. In addition, pursuant to *paragraph (d)*, any person has the right to obtain copies of documents relating to his data, and, eventually, to require the amendment and correction of such data. However, the *Law* provides in *paragraphs (j)* and *(k)*, a series of exemptions, both general and specific, by which individuals have no right to enforce their *privacy* in respect of the criminal courts activity, requested by bodies of the Executive branch, or by other *Government* Agencies, such as the *CIA*.[49] Once again, considering the latter paragraphs, we can witness an uncertain boundary between the right to *individual privacy* and the right to *National security*.

The reasons for the partial failure of the *Privacy Act* are due to the rather large number of exceptions, to the absence of an independent Body, to monitor and ensure the correct application of the *Law*, and to the often vague language of its provisions, which supported the *Government* through jurisprudence, on one hand, and the adoption of non compatible policies and programs by *U.S. Agencies*, on the other hand[50].

In the meantime, though, technological developments have urged the *Legislator* to provide adjournments of the *Act*. In fact, only two years after the *Electronic Communications Privacy Act* (1986)[51], which we encountered

---

[49] Id.
[50] Hendricks E., Hayden T. and Novik J. – *Your Right to Privacy. A Basic Guide to Legal Rights in an Information Society*, Southern Illinois University Press, Carbondale, IL, 1990, page 4.
[51] *Electronic Communications Privacy Act (ECPA)*, 18 U.S.C. § 2510-22, 1986.

already, the *Computer Matching and Privacy Protection Act* (1988) came to light. This *Act* has taken steps to amend the *Privacy Act*, in particular the points 8-13 of *paragraph (a)*, as well as some of the provisions of *paragraph (e)*. The goal was to ensure a uniform procedure in data processing and, at the same time, the Constitutional principle of *due process*, through specific boards or committees, to safeguard the integrity of processed data.[52]

Later on, still protecting *privacy* at a Federal level, the *U.S. Congress* also approved specific *privacy* measures, in the fields of *video rental and sales* (1988)[53], *car drivers records* (1994)[54], *identity theft* (1998)[55], *online children privacy* (1998)[56], *spam* (2003)[57], and *video voyeurism* (2004)[58]. Specific attention was also given to the *privacy* discipline of *health* and *genetic data*. First of all, the *Health Insurance Portability and Accountability Act* was approved in 1996, in order to regulate the increasing computerization of medical records[59]. In 2008 instead, after 10 years of congressional debates, the *Genetics Information Non-Discrimination Act* (*GINA*) was approved. Approval was unanimous in the *Senate*, and definitely overwhelming in *Congress* (414 to 1). *GINA*, presented as "the first law to protect civil rights enacted by *Congress* over the past two decades"[60], expressly forbids the use of medical records by insurance companies[61].

---

[52] *Computer Matching and Privacy Protection Act*, Public Law 100-503, 5 U.S.C. § 552a, 1988.
[53] *Video Privacy Protection Act (VPPA)*, Public Law 100–618, 1998.
[54] *Driver's Privacy Protection Act (DPPA)*, Chapter 123 of Title 18 of the United States Code, 1994.
[55] *Identity Theft and Assumption Deterrence Act*, Public Law 105–318, 112 STAT. 3007, 1998.
[56] *Children's Online Privacy Protection Act (COPPA)*, Public Law 105-277, div. C, title XIII, 112 Stat. 2681-728 (15 U.S.C. 6501 et seq.), 1998.
[57] *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) ACT*, Public Law 113-121, 15 U.S. Code § 7701, 2003.
[58] *Video Voyeurism Prevention Act*, Public Law 108-495, 2004.
[59] *Health Insurance Portability and Accountability Act (HIPAA)*, Public Law 104–191, 110 Stat. 1936, 1996.
[60] Opinion of *Jeremy Gruber*, Director of the *National Workrights Institute*.
[61] *Genetics Information Non-Discrimination Act* (*GINA*), Public Law 110–233, 122 Stat. 881, 2008.

Other important acts partially regarding *privacy* are definitely the *Communications Assistance for Law Enforcement Act* (1994)[62] and the *Personal Responsibility and Work Opportunity Reconciliation Act* (1996)[63]. However, we cannot say that all the laws approved by *Congress* have been truly in favor of *privacy*. In fact, since the introduction of *National security* programs following the terroristic attacks of September 11 2001, we can point out a gradually widespread belief of the contrast between some of these programs and the *Privacy Act* itself. We will underline in particular the debate on the *Patriot Act*'s legitimacy, especially after the *Datagate* scandal, further on.

Having said this, it is not a surprise that even *Bill Gates*, during his 2007 visit to D.C., demanded a new Federal legislation on *privacy*. The *Act* of 1974 and all of its further amendments, in fact, discipline *privacy* only partially, since they concede substantial independence to individual *States*' policies on the matter, especially in private relationships among citizens. In fact, unlike the Federal Constitutional protection of *privacy*, which focuses mainly on the relationship between the *Government* and individuals, as demonstrated in the previous paragraphs, the ordinary laws of the *Federated States* aim mostly to discipline *privacy* in terms of relations between individuals.

7. Freedom of Press and *The Right to Live in Peace*

In order to understand better the limits of the *American* system, we shall see specifically the discipline of two *privacy* areas, which are very

---

[62] *Communications Assistance for Law Enforcement Act*, Public Law 103-414, 108 Stat. 4279, 1994.
[63] *Personal Responsibility and Work Opportunity Reconciliation Act (PRWOR)*, Public Law 104-193, 1996.

relevant also in *Europe*. I am referring to the *freedom of the press* and related matters, such as the so-called "involuntary fame", as well as the equally sacred *right to live in peace*, for individuals in their home.

In terms of *freedom of press*, the *North American* legal system generally forbids diffusion of private information and data of individuals, which, no matter if truthful, can ruin their reputation. However, there are some exceptions, as when the person involved expressly gives his consent. Another exception is when someone has, or aims to have, public roles in society, for example politicians. A curious case on the topic was *New York Times Co. v. Sullivan*, in which the *Court* ruled that also profoundly embarrassing news could be published, if necessary to express with awareness a political vote.[64]

A further issue, connected to the contrast between *privacy* and *freedom of press,* is when information is gathered in public places, and is therefore potentially accessible to anybody. An example was the *Sanders v. ABC* case, involving *Mr. Sanders*, broadcasted while talking with colleagues at work. While the *Courts of First Instance* and *of Appeal* ruled that the "public" place of the episode was sufficient to avoid the broadcasting company's responsibility, later on, the *Supreme Court of California* overruled them, declaring that "the mere fact that a person can be seen (or heard) by someone does not automatically mean that he is required legally to be seen (or heard) by everyone".[65]

In the same years, the connection between the *right to privacy* and the *freedom of press* came up again in *California*, in the case *Shulman v. Group Productions Inc.* (1998). The case was about a car accident and the

[64] *New York Times Co. v. Sullivan*, 376 U.S. 254, 1964.
[65] *Sanders v. American Broadcasting Companies, Inc. et al.*, 20 Cal.4th 907, 85 Cal.Rptr.2d 909, 978 P.2d 67, 15 IER Cases 385, 27 Med. L. Rptr. 2025, 1999.

subsequent images of the injured driver, transported by an ambulance, filmed and then broadcasted on TV. Again, the "public" nature of the place in which they were filmed has not avoided the *Californian Justices* to recognize the tort for damages owed from the broadcaster[66]. However, despite the rigor of the *Courts* in *California*, historically among the most progressive *States*, we must not be induced to believe that the *Federal State* laws have been uniform on the matter.

Regarding the *right to live in peace,* for individuals in their home, instead, we need to refer once more to *Warren* and *Brandeis*' conclusion, in their "The Right to *Privacy*", that "the Common law has always recognized a man's house as his castle".[67] In fact, if on one hand, as we pointed out before, there is a Constitutional protection of the "freedom of expression" (*First Amendment*), the *U.S. Supreme Court* has been protecting at the same time "the right to be let alone."[68] Among the consequences of this protection, were the ban of "door to door" salesmen, the ban on the use of loudspeakers in residential areas, and the right to refuse to receive mail from unknown senders.

Therefore, as stated by the *Court* in the 1970 *Rowan v. Post Office Department* case, if "making the householder the exclusive and final judge of what can go through his door undoubtedly has the effect of preventing the free flow of ideas", never the less, "there is no Constitutional provision that forces individuals to hear or receive unsolicited communications, whatever the content"[69], thus confirming the above-mentioned theory of *Warren* and

---

[66] *Shulman v. Group Productions Inc.,* 74 cal. Rpt. 2d 843, 1998.
[67] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 220.
[68] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 195.
[69] *Rowan v. Post Office Department,* 397 U.S. 728, 1970.

Brandeis.[70] This orientation was confirmed also in the 1988 *Frisby v. Schultz* case: "domestic privacy is the utmost value for a free and civilized society" because "one is not required to welcome an unwanted speech into his home.[71]"

8. Digital *Privacy*

In light of the continuous technological developments, already referred to earlier, however, this physical domestic protection, represented by closing "the front entrance" of the house[72], is not enough nowadays. In fact, the feeling of danger connected to the loss of *privacy* has spread in our society[73]. While until a few years ago the concern was the property of a narrow band, more aware and informed[74], the trend has now changed, involving more layers of the population[75]. Pointing out the tons of spams and junk emails, which invade our computers everyday, is, therefore, sufficient to understand why we need to embrace the concept of *digital privacy* now.

Further more, technological innovations, such as the advancement of information technology, have provided powerful tools to invade the individuals' personal sphere[76], otherwise destined to remain intimate[77]. The time and costs required to collect and to process data have been reduced

---

[70] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 195.
[71] *Frisby v. Schultz,* 487 U.S. 474, 1988.
[72] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 220.
[73] Regan P. M. – *Legislating Privacy: Technology, Social Values, and Public Policy*, The University of North Carolina Press, Chapel Hill, NC, 1995, page 50.
[74] Harris L. and Westin A. F. – *The Dimensions of Privacy. A National Opinion Research Survey of Attitudes toward Privacy*, Garland Publishing, New York, NY, 1981, page 3.
[75] Smith H. J. – *Managing Privacy. Information Technology and Corporate America*, The University of North Carolina Press, Chapel Hill, NC, 1994, page 1.
[76] Freedman W. – *The Right to Privacy in the Computer Age*, Quorum Books, New York, NY, 1987, page 93.
[77] Regan P. M. – *Legislating Privacy: Technology, Social Values, and Public Policy*, The University of North Carolina Press, Chapel Hill, NC, 1995, page 10.

significantly, encouraging and stimulating the possible association of a large amount of information with a theoretically indefinite number of specific subjects[78].

Moving from the knowledge of all the issues arisen because of the implementation of new technologies: databases, biometric identification devices and, in general, the world of interpersonal relationships mediated by the Internet, it seems obvious that *privacy* related problems need to be addressed with the same level of information made available by those technological means.

Internet, in fact, is allowing us to not only to communicate, but also to obtain information, perform business transactions, and to visit virtual places. Further more, it allows third parties not only to read the communication between two or more people, but also to discover the information sought by a person online, to see his financial transactions, and to become aware of the interests of that person[79].

The invasion of *individual privacy*, therefore, has never been so widespread and tends to increase dramatically. The development of technology is largely responsible for this situation[80], particularly with the application of computers to data processing, which allows instant access to huge amounts of information, and the ability to collect real-time data and process them in a short time[81].

The two major technologies, which contributed to a greater social interaction and information diffusion, are, in fact, definitely *Databases* and

---

[78] Lugaresi N. – *Internet, Privacy e Pubblici Poteri Negli Stati Uniti*, Seminario Giuridico della Università di Bologna, Milano, Giuffrè Editore, 2000, page 9.
[79] Id.
[80] Rosenberg J.M. – *The Death of Privacy*, Random House, New York, NY, 1969, page 143.
[81] Lugaresi N. – *Internet, Privacy e Pubblici Poteri Negli Stati Uniti*, Seminario Giuridico della Università di Bologna, Milano, Giuffrè Editore, 2000, page 10.

the *Web 2.0*. The striking technological advances developed in the fields of *Databases* and of the *Web 2.0* must not, however, make us lose sight of their crucial differences. In regards to *Databases*, the legal boundary between public and private is more significant. It is the case, for example, of search engines such as "Google", which are limited by the *Government*'s protection systems. The most significant feature of the *Web*, instead, is having contributed to the uncertain range of legal and political power on the matter, of Sovereign States. Therefore, it might be useful to analyze the problem of *Database* management first, and the one related to the side effects of the *Web*, afterwards.

9. Database Management

Regarding *Database* management, what really matters in terms of *privacy* policy is the utility of these data: whether collected for "*National security* reasons", rather than for "pure commercial purposes". In the first case, needed by Public Authorities, which justify and legalize the creation of increasingly powerful *Databases*, it seems obvious that the consent of the parties concerned is not necessary for the data's collection. As the provisions of the *Privacy Act* make clear though, the goal is to ensure that the enormous amount of personal information under public control remains in some way under the control of the person concerned, through the *right of access and of rectification*, guaranteed by the entire Constitutional system, and especially by the rulings of the *Supreme Court*.

In the case *United States v. Department of Justice v. Reporters Committee for Freedom of the Press* (1989), for example, the *Supreme Court*

ruled that the central purpose of the *FOIA*[82] is to ensure that the activities of the *Government* are open the watchful eye of public scrutiny, and not to disclose the information on private citizens, which casually happens to be kept in the archives of the *Government*. "[83] The *Freedom of Information Act* also applies to relevant information for Governmental activities, while individuals' purely personal information should not be disclosed, because it would go beyond the scope of the right of that *Law*[84]. In the case that data is collected for commercial purposes, instead, which therefore involves banking, economic, financial, industrial and commercial organizations, consensus, at least in principle, becomes crucial.

In fact, no matter the presence of *Statutory* protections of electronic surveillance of businesses, mail fraud, video privacy, cable communications, phones and the protection of minors on the Internet, many of the problems that have arisen in the *U.S.* because of *privacy* actually depend on the specific *North American* "way of life". Beyond the existing problem of inappropriate manipulation of data, produced without the consent of the individual it concerns, people often give their data to the other party their selves, in order to obtain a credit, a loan or a deferred sale. Examples of inappropriate *database* manipulation were *Sony-BGM*'s use of "spyware" in 2005, and *Symantec*, popular for its *Norton Security Suite*, using "root-kit" to hide files in the computers of its clients.[85]

---

[82] *Freedom of Information Act (FOIA),* 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, 1966.
[83] *United States v. Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749, 1989.
[84] Schwartz P. M. and Reidenberg J. R. – *Data Privacy Law. A Study of United States Data Protection*, Michie Law Publishers, Charlottesville, VA, 1996, page 108.
[85] Holtzman D.H - *Privacy Lost: How Technology Is Endangering Your Privacy,* San Francisco: Jossey-Bass, 2006, pages 206 – 207.

10. World Wide Web

The other main problematic of *digital privacy*, is definitely the *World Wide Web*. If *Warren* and *Brandeis* had suggested to "close the front entrance" of the house,[86] to avoid deception, fraud, espionage, defamation, and so on, the Internet's diffusion brought to light several other offenses, such as cloning or identity theft, virus infection, electronic insulation, software corruption or virtual forms of complicity. These offenses, of course, cannot be prevented simply by closing "the front entrance" of the house[87].

So far, therefore, the *U.S.* has reacted with the approval of applicable *Federal* or *State* laws, which are designed to discourage similar behavior, on the basis of physical sanctions threatened to the authors of spamming, phishing, spyware, and anything of the kind. An example of the legislation on the matter is the *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) ACT* of 2003, *15 U.S. Code § 7701*[88]. Among the most severe *State* legislation, instead, a good example is the *Californian Code on Business and Professions*, § *17538.4*, which imposes on the transgressors fines up to $ 25,000 per day[89].

In fact, like many of the problems that have arisen with the public management of *databases*, which have to deal with the attacks of hackers as well, the issue of "side effects of the Internet" definitely goes beyond the traditional legal and political boundaries of *Sovereign States*, suggesting forms of international cooperation. Therefore, we will come back to these

---

[86] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 220.
[87] Id.
[88] *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) ACT*, Public Law 113-121, 15 U.S. Code § 7701, 2003.
[89] *Californian Code on Business and Professions*, § 17538.4, 2003.

issues, which of course do not concern only the *United States*, once we examine similar problems that arise from the *European* model of *privacy*.

11. Privacy and *Terrorism, and* the *USA PATRIOT Act*

After the historical analysis of the *American privacy* legislation, we must now move on to what has been the field of greatest importance in the past decades in terms of the *privacy-security* relation, which is the discipline of *privacy* in relation to terrorism. This imminent focus should finally help us evaluate the "uncertain" *boundary* between *individual privacy* and *national security* in the *U.S.*, core topic of my thesis.

First of all, we can shift our attention to the particularly emblematic area of *flight safety*, in order to clarify some of the serious dilemmas that counter terrorism emergency legislation has caused regarding *privacy*, for example. In fact, for more than understandable reasons, one of the first measures taken by the *U.S.* after the *Twin Towers Attack* in September 2001, was a program for the protection of air transportation controlled by the *Department of Homeland Security*[90], which created a specific institution, namely the *Transportation Security Agency*[91], according to the reforms introduced by the *Patriot Act*.

The *USA PATRIOT Act* is an Act of *Congress* that was signed into law by President *George W. Bush* on October 26, 2001. The title of the *Act* is a ten-letter acronym (*USA PATRIOT*) that stands for "Uniting (and) Strengthening *America* (by) Providing Appropriate Tools Required (to) Intercept (and)

---

[90] The Department was established on March 1, 2003, replacing the previous *Immigration and Naturalization Service*.

[91] The Agency was established on November 19, 2001 with the *Aviation and Transportation Security Act,* and depends now from the *Department of National Security*, since its establishment, on March 1, 2003.

Obstruct Terrorism"[92]. It is commonly referred to simply as the *Patriot Act*.[93] This *Law*[94], made up of ten sections, was broad and brought many and considerable changes to the previous legislation, intervening with useful tools in order to make the fight against terrorism easier and more effective. Among the most important provisions included were those aimed at giving more powers to the investigating bodies, that acquired greater freedom of movement in the search for evidence, also through interceptions collected with special *privacy* standards.

Further more, the *Patriot Act* amended the *Bank Secrecy Act*[95] and the legislation on money laundering, both at a National and International level. It also changed the immigration laws to prevent foreign terrorists entering into the *Country*, and intervened on behalf of victims of crimes linked to terrorism, of their families and of the rescue workers. The *Act* created new offenses and increased penalties for existing crimes of terrorism. Beyond this, *Public Law 107-56* significantly enhanced the action of Federal intelligence agencies, including the *CIA*[96]. In fact, the strategy was to coordinate and share data between the directly involved organizations, given the disorganization and failed synergy between the activities of the *CIA* intelligence and the investigations conducted by the *FBI*, that emerged from the "*9/11 Attack*".

However, no matter if the *USA PATRIOT Act* was approved by large majorities in 2001, both in the *U.S. Senate* and *House of Representatives*, it gave birth to several controversies. Some parts of the *Act* were invalidated or

---

[92] "Patriot Act", *Wikipedia*.
[93] Id.
[94] *USA PATRIOT Act*, Public Law 107-56, 2001.
[95] *Bank Secrecy Act*, Public Law 91-508, 1970.
[96] *USA PATRIOT Act*, Public Law 107-56, 2001.

modified by successful legal challenges, based on Constitutional infringements of civil liberties. *Public Law 107-56* had also many sunset provisions, but most of them were reauthorized by the *USA PATRIOT Improvement and Reauthorization Act* (2005),[97] and by the *USA PATRIOT Act Additional Reauthorizing Amendments Act* (2006)[98]. These reauthorizations included amendments to the original *USA PATRIOT Act*, and also to other Federal laws[99]. Also President *Barack Obama*'s recently extended the action of some crucial measures of the *Patriot Act*, in 2011[100], but there have been other relevant *U.S.* laws related to the *privacy-terrorism field*, before then.

12. The *Matrix Program*

In 2003, for example, the *Department of Homeland Security* and the *Department of the Treasury* funded, with eight million dollars, the *Matrix Program*, specifically the *Multistate Anti-Terrorism Information Exchange*[101]. In this project of a *database* for the protection of the National territory, beyond the *Federal Government*, also thirteen *States* of the *Union* participated, including the main ones: *California*, *Texas* and *New York*. *Matrix* allowed the use of information made available by commercial databases for *National security*, clearly derogating the 1974 *Privacy Act*[102]. The operational phase of this project started in July 2003, but no special *privacy* measures were taken[103].

---

[97] *USA PATRIOT Improvement and Reauthorization Act*, Public Law 109–177, 2005.
[98] *USA PATRIOT Act Additional Reauthorizing Amendments Act*, Public Law 109–178, 2006.
[99] "History of the Patriot Act", *Wikipedia*.
[100] "Patriot Act", *Wikipedia*.
[101] "Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project", *Privacy Office - U.S. Department of Homeland Security*, Washington D.C., 2006.
[102] *Privacy* Act, Public Law 93-579, 88 Stat. 1897, in 5 U.S.C. n 552, 1974.
[103] "Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project", *Privacy Office - U.S. Department of Homeland Security*, Washington D.C., 2006.

However the *Matrix Program* was criticized by many associations, and, above all, by the *American Civil Liberties Union (ACLU)*. In 2004, it was discovered that *Matrix* allowed *Federal Agencies* to register indiscriminately citizens, with data relating to criminal records, driver's licenses, vehicle registrations, court documents, real estate property registers, professional and commercial licenses, personal phone directories, various types of tickets, relatives' names, and also to National health service numbers, in order to "protect" *National security*[104]. Further more, only 2.6 percent of the cases filed were later proven to deal somehow with terrorist activities.

Anyway, after months of criticism, protests and harsh civil strikes, the *American Civil Liberties Union* finally announced, in April 2005, that the *Matrix* project was abandoned by the *Bush* administration, for the inefficiency of the initiative, and for the first admissions of non-compliance to *privacy* laws[105]. This was definitely a great lesson of democracy. The *ACLU* had done its job as a "watchdog" of justice. However, other *profiling* and *data mining* programs were funded later on.

13. Flight Safety Programs

In 2003, also the *Computer Assisted Passenger Pre-screening System II*[106] entered into force. It was a system that used passengers' data, provided by the flight company *Delta*, and crossed it with the data provided by commercial databases, in order to establish the specific risks of each

---

[104] Staff - "MATRIX: Myths and Reality", *American Civil Liberties Union, www.aclu.org*, 2004.

[105] Id.

[106] "The *Computer-Assisted Passenger Prescreening System* (often abbreviated *CAPPS*) is a counter-terrorism system in place in the United States air travel industry. The United States Transportation Security Administration (TSA) maintains a watchlist, pursuant to 49 USC § 114 (h) of "individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety." The list is used to pre-emptively identify terrorists attempting to buy airline tickets or board aircraft traveling in the United States, and to mitigate perceived threats" ("Computer-Assisted Passenger Prescreening System", *Wikipedia*).

passenger: green for low risk, yellow in case of additional controls requests and, finally, red for those passengers judged to be at a high risk.

However, in August 2004, the second-generation *Computer Assisted Passenger Prescreening System* was replaced by the *Secure Flight Program*, administered by the *United States Transportation Security Administration (TSA)*, under the *Department of Homeland Security*'s control[107]. Its first goal was to complete the list of passengers flying in the *U.S.* since June of that year, integrating the information with the one of commercial databases of some private companies, such as *Acxiom*, *Insight America* and *Qsent*, purchased through the subsidiary *Eagle Force*, based in *Virginia*[108]. Among the required information of passengers, beyond their names and the names of their spouses, were their sex, address, date of birth and, of course, their social *security* number.

Differently from what had occurred with the *Matrix* project, though, in November 2004, the *Department of Homeland Security*, through the *Transportation Security Agency*, published a report, in which it guaranteed that the *Agency* would protect the *privacy* of individuals, during its anti-terrorist controls[109].

Anyways, three months after the closure of the *Matrix Program* (April 2005), in the same climate of protests and concerns, on July 22 2005, the *Government Accountability Office*, sent a letter to the *Congress* in *Washington*, accusing the *Transportation Security Agency* of actually violating the *Privacy*

---

[107] "Secure Flight", *Wikipedia*.
[108] "Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations", *Privacy Office U.S. Department of Homeland Security,* Washington D.C., 2006.
[109]"Notice of Final Order for Secure Flight Test Phase; Response to Public Comments on Proposed Order and Secure Flight Test Records", *Federal Register*, Vol. 69, § 219, "Notices", 65619 – 65627, *Department of Homeland Security, Transportation Security Administration* [Docket No. TSA–2004–19160], November 15 2004.

Act, since "Federal Agencies are required to explain the way in which the information of the persons concerned is collected, maintained, used, and disseminated", while the *TSA,* beyond not ensuring the protection provided by the *Law*, and with all due respect to the declarations of the report published in November 2004 mentioned earlier[110], kept using specialized firms, to obtain additional data on passengers[111].

In February 2006, the Head of the Agency, *Kip Hawley*, was cornered on this issue, so he announced before the *Senate Committee on Commerce, Science and Transportation*, that the *Program* was suspended indefinitely[112]; and, later on, in the *Report to the Public on the Transportation Security Agency's Security Flight Program and Privacy Recommendations*, he admitted the illegal use of commercial databases, which, no matter the cost of 140 million dollars, beyond at least 80 extra million dollars to refine the *Program*, still had 144 *security* flaws[113].

However, in August 2007, shortly after the controversial agreement on *PNR data* with the *European Union*, the *Department of Homeland Security* announced the resumption of the project, which at first was supposed to be suspended until 2010. Although, on one hand, Federal Representatives promised that the new *Security Flight Program* would not use commercial databases, scores for passengers, neither would it try to predict their

---

[110] Id.

[111] "Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public", Congressional Committees, *United States Government Accountability Office*, Washington, July 22, 2005.

[112] "Statement of Kip Hawley, Assistant Secretary of the *Transportation Security Administration*, before the *Subcommittee on Homeland Security Committee on Appropriations United States House of Representatives*", *United States Department of Homeland Security Transportation Security Administration*.

[113] "Report Says TSA Violated Privacy Law", By Ellen Nakashima and Del Quentin Wilber, *Washington Post,* Friday, December 22, 2006.

behavior, on the other hand, these declarations confirmed some of the most evident violations of *privacy* occurred in recent years.

According to the *TSA* own website, the *Secure Flight* has now adjourned its *privacy* protection: "Ensuring the *privacy* of individuals is a cornerstone of *Secure Flight*. *TSA* developed a comprehensive *privacy* plan to incorporate *privacy* laws and practices into all areas of *Secure Flight*. The *Program* worked extensively to maximize *individual privacy*. In addition to assuring compliance and reinforcing its commitment to protecting *privacy*, *Secure Flight* created an environment dedicated to guaranteeing its *privacy* mission that is front and center every day"[114]. Therefore, at least in flight related anti-terrorism controls, hopefully, the *Privacy Act* infringements of the past should not be perpetrated again.

14. The *Patriot Sunsets Extension Act*

Of course, the above legislation was based on the 2001 *USA PATRIOT ACT*, briefly described earlier[115]. The *Law*, in a nutshell, reduced or eliminated many of the restrictions for *Government* Agencies, in their telephone communications' interceptions and in their medical and financial data digital management activities. It also increased the discretion and the powers of the *Government* in dealing with terrorism suspects outside of the *U.S.* borders and thus, actually compressed certain *rights* and *civil liberties* in the name of *National security*. The bulk of these measures came into force permanently. However, some of them, because of their exceptional nature, must be periodically revised and extended, otherwise cease to have value. As already mentioned, President *Barack Obama* extended three of these

[114] "Secure Flight Program", *Transportation Security Administration*, www.tsa.gov.
[115] *USA PATRIOT Act*, Public Law 107-56, 2001.

measures until 2015, when he signed the *Patriot Sunsets Extension Act*, , directly from *Paris,* on May 26 2011[116].

One of the *Sections* of the *Act*, extended in 2011, allows *Government* Agencies to conduct wiretaps of people suspected of terrorism, and not only on specific phone lines, thus allowing to control various phone lines in different places. Another *Section* gives the *Government* easy access to a wide range of data of suspected terrorists: personal, medical, and financial, above all. The third *Section*, extended in 2011, allows *Government* Agencies to investigate the so-called "lone wolves", persons suspected of terrorism, but apparently with no contacts or affiliations with terrorist groups.

15. Critics to the *USA PATRIOT ACT* and its *Extension Acts*

Many in the *U.S.*, both Democrats and Republicans, have criticized heavily the *Patriot Act* and its *Extension Acts*. However, in terms of *privacy*, and therefore among the criticisms relevant for our study, is the evident contrast with the ban of "unreasonable searches and seizures", provided by the *Fourth Amendment*. For this reason *American* media, at the time of the debate, brought up what Justice *Robert H. Jackson*, the former chief *United States* Prosecutor at the *Nuremberg* trials, had written in 1949: "Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary *Government*".[117]

Further more, *Immigration Authorities* have argued that the criterion of "reasonable grounds to believe", according to which the Attorney General authorizes the detention of foreigners, corresponds substantially to the

---

[116] *PATRIOT Sunsets Extension Act*, S. 1038 (112th), 2011: This bill was introduced on May 19, 2011, in a previous session of Congress, but was not enacted.

[117] Gentili G. - "Stati Uniti. Estesa sino al 2015 l'efficacia del Patriot Act tra crescenti critiche circa la possibile violazione di diritti fondamentali garantiti dalla Costituzione", *DPCE online,* Numero 3, 2011.

"reasonable suspicion" parameter, required by the *Fourth Amendment* for a legitimate detention or a search warrant[118]. However, the fact that "mere suspicion" is not sufficient to justify a proper arrest, in the field of Criminal law, while it is sufficient for an indefinite detention, when it comes to enforcing immigration laws, is definitely not reasonable[119].

Beyond this, a major critique of the *Patriot Act* is the *American* Scholar *Amitai Etzioni*, who proposed to distinguish the surveillance technologies between "liberalizing" and "public-protective", in his essay on the patriotism of the *Patriot Act*[120]. Among the first, he included cell phones, emails and cryptographic techniques; while he included the programs used by the *FBI* among the latter. *Etzioni* believes that if the first kind of technologies, considering the new horizons of interpersonal communication, have often made inadequate forecasts, aimed at controlling the social order, the second kind, instead, have been mostly used to narrow the space of action, offered by the "liberalizing" technologies[121].

A good example, to better understand his theory, is the old *North American* legislation on the control of crime and road safety, *Omnibus Crime Patrol and Safe Streets Act* (1968)[122]. In fact, it required the permission of the *Court* for each interception, specifying the location of the device, typically the

---

[118] "The Fourth Amendment to the U.S. Federal Constitution provides: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (*US Constitution, Fourth Amendment*).

[119] Bassu C. - "La legislazione antiterrorismo e la limitazione della libertà personale in Canada e negli Stati Uniti", in Groppi T. - *Democrazia e terrorismo. Diritti fondamentali e sicurezza dopo l'11 settembre 2001*, Editoriale Scientifica, Napoli, 2006.

[120] Etzioni A. - *How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism*, Taylor & Francis, 2004, page 45.

[121] Id.

[122] *Omnibus Crime Control and Safe Streets Act*, Public Law 90–351, 82 Stat. 197, enacted on June 19, 1968, codified at 42 U.S.C. § 3711.

phone to intercept, and the reasons why the interception of the communications, made through that particular medium (more often a computer, nowadays) could lead to the evidence of a crime[123].

In 2001, however, the *Patriot Act* suggested to extend the investigative powers of the Judges to a Federal level, with the aim of safeguarding *National security*[124]. This means that if once the orders to scour the electronic records were valid only for the jurisdiction of that particular *Court* (in *New York*, *Los Angeles*, etc.), since the *Patriot Act*, the order of the *Court* covers the entire National territory. According to many, the definitions listed in *Section 802* of the *Patriot Act* may also comprehend many forms of civil disobedience[125].

Among other apparent violations of *civil liberties* connected to the measures of the *Patriot Act* there are three main ones. First of all, *Section 802* of the *Act* introduced *domestic terrorism*: "acts dangerous to human life that are a violation of the Criminal laws of the *United States* or of any *State*", aimed to "(i) intimidate or coerce a civilian population; (ii) influence the policy of a *Government* by intimidation or coercion; or (iii) to affect the conduct of a *Government* by mass destruction, assassination or kidnapping" (...) that occur primarily within the jurisdiction of the *United States*"[126]. Secondly, *Section 215* of the *Patriot Act* added the new *§ 501* to the *Foreign Intelligence Surveillance Act*[127], which states that the *FBI* can obtain information from "third parties", with a simple written request, therefore no judicial authorization is needed, in cases involving "*National security*"[128].

---

[123] Id.
[124] *Section 216*, *USA PATRIOT Act*, Public Law 107-56, 2001.
[125] Solove D., Rotenberg M. and Schwartz P.M. – *Privacy, Information and Technology*, Aspen, New York, 2006, page 108.
[126] *Section 802, USA PATRIOT Act*, Public Law 107-56, 2001.
[127] *Foreign Intelligence Surveillance Act (FISA)*, Public Law 95–511, 92 Stat. 1783, 50 U.S.C., 1978.
[128] *Section 215*, *USA PATRIOT Act*, Public Law 107-56, 2001.

Finally, *Section 213* of the *Patriot Act* allows a late disclosure of the evidence, against the suspected person, in the judicial process. The suspect, therefore, is aware of this evidence only in the course of his trial, unlike "normal" cases, in which the probative evidence must be notified to him as soon as it is collected.

However, as the Italian *Comparative Privacy Law* Professor of *Georgetown University, Ugo Pagallo,* points out in his "Lo Stato della Privacy", the shock provoked in the *U.S.* by the *Patriot Act*'s measures is mostly due to the fact that many of the dispositions of the precedent *Foreign Intelligence Surveillance Act* (1978), regarding only foreigners or "aliens", "are now applicable to *American* citizens too"[129]! The fundamental difference that, from his point of view, distinguishes the *Patriot Act* from the so-called *FISA*, is to expand the spectrum of data "intelligence", relating to foreign affairs. Therefore, for the *Patriot Act*, a simple "significant reason" is enough to begin investigating a suspected subject[130].

16. Boundaries between *Privacy* and *Security* in the *U.S.*

In order to evaluate the *boundary* between *privacy* and *security* in the *U.S.*, we have to consider, first of all, the lack of general rules governing *privacy* "directly", at a Constitutional level, and also the limits of the sectorial emergency legislation, such as the *Patriot Act*, evidenced so far. Further more, considering the often-insufficient importance attributed to *privacy* among the fundamental rights, and also the missing strong Federal *privacy* policy, since 1974, it is not hard to evaluate that the needs of *National security* have in many ways prevailed on those of *individual privacy*, in the

[129] "Lo Stato della Privacy", Pagallo U. - *La Tutela della Privacy Negli Stati Uniti D'America e in Europa*, Giuffrè Editore, 2008, page 25.
[130] Id.

U.S., so far. We will now proceed to analyze the *European* legislation on the matter, in the next *chapter*, in order to compare the two systems, further on.

Chapter II

Individual Privacy and *National Security*

In the *European Union*

17. Europe's Non-Federation

Unlike the *United States of America*'s, the *European Union*'s legal system is not, as of today, a Federal system. According to the classic definition of the *European Court of Justice*, it is rather "a sort of new genre in the history of International law"[131], in favor of which *Member States* have surrendered their sovereignty, at least in certain areas. What constitutes the novelty of the genre, however, is still a controversial issue, to say the least. For example, some argue whether it is a "multi-level" Constitutional system[132], a "mixed" legal system of democratic and technocratic element[133], a peculiar version of *European* Federalism[134], or a new variant of the medieval *jus commune*[135]. Finally, some, focusing on the absence of original jurisdiction, argue that the model of *Union* law "does not stray too much from the model of standard International law organizations, after all" [136].

---

[131] *Case 26-62,* "NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration". Reference for a preliminary ruling: Tariefcommissie - Netherlands, Judgment of the Court of 5 February 1963.

[132] Pernice I. - "Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitutionalism in Making Revisited?", *Common Market Law Review*, 1999, pages 703 - 750.

[133] *MacCormick N. - Questioning Sovereignty. Law, State, and Nation in the European Commonwealth, Oxford University Press, Oxford, 1999.*

[134] *Weiler J.H.H. - The Constitution of Europe. "Do the New Clothes Have an Emperor?" and Other Essays on European Integration, Cambridge University Press, Cambridge, 1999.*

[135] *Coing H. - Von Bologna bis Brussels: Europäische Gemeinsamkeit, Gegenwart und Zukunft, Kölner Juristische Gesellschaft, IX, Bergish Gladbach-Köln, 1989.*

[136] Schilling T. - "The Autonomy of the Community Legal Order – An Analysis of Possible Foundations", *Harvard International Law Review*, 37 Harv. Int'l L.J. 389, Spring, 1996, pages 389 - 410.

However, abandoning the field of general theory of law and returning to the issues of *privacy*, we can affirm that the structure of the *Union*'s legal system is, never the less, similar in many ways to a Federal system's one[137]. Beyond Constitutional sources of law (no matter the abortion of a *Constitutional Treaty Draft* in 2005), there are also other general rules for the protection of *privacy* in *Europe*, in the sense that all *Member States* are required to adopt them. Further more, there is a widespread control of the legality of acts, similar to that existing in the *U.S.*, mentioned in *Chapter I*.

This enables *National Courts* not to apply, in certain circumstances, the law of their *Countries*, in order to resolve the dispute in accordance with *Union* law[138], and also to plea the *Court of Justice*, pursuant to *Article 267* of the *Treaty on the Functioning of the European Union (TFEU)*, whether doubts regarding the meaning of the *Union*'s provisions arise[139].

The aim is to ensure in this way the full uniformity of legal principles and provisions of the *Union* law, in all the *Member States*. As we have done previously for the *United States*, therefore, we must analyze the Constitutional sources of *European Union* law first, and the ordinary legislation and regulations, afterwards.

18. EU Constitutional *Privacy* Law

The *European* system of Constitutional guarantees, protecting the right to *privacy*, may be conceived as a complex pattern made of *Union*

---

[137] *Weiler J.H.H. - The Constitution of Europe. "Do the New Clothes Have an Emperor?" and Other Essays on European Integration, Cambridge University Press, Cambridge, 1999.*

[138] *Case 106/77* – "Amministrazione delle Finanze dello Stato v Simmenthal SpA". - Reference for a preliminary ruling: Pretura di Susa - Italy. Discarding by the national court of a law contrary to Community law". ECJ, March 9 1978.

[139] "Preliminary ruling", provided by *Article 267* of the *Treaty on the Functioning of the European Union (TFEU)*, former *Article 234* of the *Treaty establishing the European Economic Community (TEEC).*

provisions, International declarations, common Constitutional traditions of *Member States*, and jurisprudence of the *European Court of Justice*[140]. In fact, when the *European Economic Community (EEC)* was founded, with the agreements signed in *Rome* in 1957, in order to create a common market, the *Treaty* did not contain specific provisions on human rights[141]. However, the absence of these provisions was balanced by the *European Court of Justice*'s admirable effort of extensive interpretation, of individual National provisions, since the beginning of the seventies.

Though, between the eighties and the nineties, when the *Universal Declaration of Human Rights (UDHR)*[142] and the *European Convention on Human Rights (ECHR)*[143] were formally transposed in *Community* legislation, this did not depend exclusively on the persistent jurisprudence of the *ECJ*. In fact, the full and formal recognition of human rights within the *EU*

---

[140] This pattern has been presented in the literature as a system with more levels, that escapes the traditional theory of Kelsen, that identifies the Legal Order into the "center" of regulatory powers. In fact, since Community law emerged through an act of renunciation, of the member states to their sovereignty , albeit limited, the logic of this theory must not be read only from as a threat of coercive measures, but also in the opposite direction, "from the bottom to the top", or in a "horizontal" way. This thesis is proposed and analyzed thoroughly by Bilancia P. and Pizzetti F.G., in their book (*Aspetti e problemi del costituzionalismo multilivello*, Giuffrè, Milano, 2004). Also Sabino Cassese had proposed the '"Community harmonization of national laws" (from top to bottom), the "integration of legal traditions of constitutional law" (from bottom to top), and the "choices between different legal orders allowed by the mutual recognition "(the horizontal relation), in his book (*La crisi dello stato*, Laterza, Roma-Bari, 2002, page 130). Finally, also Ugo Pagallo shares the same theory (*Teoria giuridica della complessità. Dalla 'polis primitiva' di Socrate ai 'mondi piccoli' dell'informatica. Un approccio evolutivo*, Giappichelli, 2006, pages 136-137).

[141] *Treaty establishing the European Economic Community (TEEC)*, Rome, 1957.

[142] "The *Universal Declaration of Human Rights (UDHR)* is a declaration adopted by the United Nations General Assembly on 10 December 1948 at the Palais de Chaillot, Paris. The Declaration arose directly from the experience of the Second World War and represents the first global expression of rights to which all human beings are inherently entitled" (*"*Universal Declaration of Human Rights*", Wikipedia*).

[143] "The *European Convention on Human Rights (ECHR)* (formally the *Convention for the Protection of Human Rights and Fundamental Freedoms*) is an international treaty to protect human rights and fundamental freedoms in Europe. Drafted in 1950 by the then newly formed Council of Europe, the convention entered into force on 3 September 1953. All Council of Europe member states are party to the Convention and new members are expected to ratify the convention at the earliest opportunity" ("European Convention on Human Rights", *Wikipedia*).

Constitutional *Treaties* was also highly symbolic, for the transition from the *European Economic Community (EEC)* to the *European Community* (EC)[144], at first, and for the establishment of the *European Union*, occurred when the *Maastricht Treaty* came into force (November 1 1993), afterwards[145].

Finally, this long process resulted in the solemn proclamation of the *Charter of Fundamental Rights of the European Union*, on December 7 2000 in *Nice*, signed by the *Presidents* of the *Commission*, of the *Council* and of the *European Parliament*[146]. The *Charter* is an essential reference point for the Constitutional right to *privacy* in *Europe*[147].

19. The *Charter of Fundamental Rights of the European Union*

Among the fundamental rights of the *European Union* in terms of *privacy* is surely *Article 7* of the *Charter*, which imposes "respect for private and family life of everyone"[148], and, therefore, partially reproduces *Article 8*

---

144 "The *Merger Treaty* (or *Brussels Treaty*) was a European treaty which combined the executive bodies of the *European Coal and Steel Community (ECSC)*, *European Atomic Energy Community (Euratom)* and the *European Economic Community (EEC)* into a single institutional structure. The treaty was signed in Brussels on 8 April 1965 and came into force on 1 July 1967" ("Merger Treaty", *Wikipedia*).

145 "The *Maastricht Treaty* (formally, the *Treaty on European Union* or *TEU*) undertaken to integrate Europe was signed on 7 February 1992 by the members of the *European Community* in Maastricht, Netherlands. On 9–10 December 1991, the same city hosted the *European Council* which drafted the treaty. Upon its entry into force on 1 November 1993 during the *Delors* Commission, it created the *European Union* and led to the creation of the single European currency, the euro. The Maastricht Treaty has been amended by the treaties of Amsterdam, Nice and Lisbon" ("Maastricht Treaty", *Wikipedia*).

146 "The *Charter of Fundamental Rights of the European Union* enshrines certain political, social, and economic rights for *European Union (EU)* citizens and residents into EU law. It was drafted by the *European Convention* and solemnly proclaimed on 7 December 2000 by the *European Parliament*, the *Council of Ministers* and the *European Commission*. However, its then legal status was uncertain and it did not have full legal effect until the entry into force of the *Treaty of Lisbon* on 1 December 2009". ("Charter of Fundamental Rights of the European Union", *Wikipedia*).

147 "Il Modello europeo della privacy", Pagallo U. - *La Tutela della Privacy Negli Stati Uniti D'America e in Europa*, Giuffrè Editore, 2008, page 115.

148 *Article 7* - "Respect for private and family life", *Charter of Fundamental Rights of the European Union*.

of the *European Convention on Human Rights (ECHR)*[149]. However, the *Nice Charter* goes beyond the *Convention*'s protection of the "private life of individuals", as a fundamental human right. In fact, *Article 8* of the *Charter* protects the right to *privacy*, specifically in terms of "personal data protection"[150]. This *Article* is composed of three *Sections*. First of all, *Section 8.1* provides the general right "to personal data protection"[151]. Further more, *Section 8.2* determines that said data must be processed "for specified purposes", and "on the basis of the individuals' consent". It also provides the "right to access the data" and, eventually, the "right to data rectification"[152]. Finally, *Section 8.3* establishes "an independent Authority", in order to guarantee these rights[153].

However, no matter the consideration of the right to *privacy* as a fundamental right of men, evidenced in the *Charter*, there have been many doubts on the binding force of its provisions, since the failed attempt of a *Constitutional Treaty Draft* in 2005, which included also the *Charter*'s provisions. Before moving on to the other *EU* Treaties, therefore, we must analyze the *Court of Justice*'s jurisprudence, a key element of the *EU* Constitutional sources, as mentioned earlier, and persistent enough to clear the doubts on the *Charter*'s validity.

---

[149] *Article 8* – "Right to respect for private and family life", *Convention for the Protection of Human Rights and Fundamental Freedoms*.
[150] *Article 8* – "Protection of personal data", *Charter of Fundamental Rights of the European Union*.
[151] *Section I, Article 8* – "Protection of personal data", *Charter of Fundamental Rights of the European Union*.
[152] *Section II, Article 8* – "Protection of personal data", *Charter of Fundamental Rights of the European Union*.
[153] *Section III, Article 8* – "Protection of personal data", *Charter of Fundamental Rights of the European Union*.

20. Jurisprudence of the *European Court of Justice*

Since the 1970 *Internationale Handelsgesellschaft* case[154], the 1974 *Nold* case[155], and the 1979 *Hauer* case[156], the *Court* has held that "the protection of human rights is an integral part of *Community* law," referring to the common Constitutional traditions of the *Member States*, and also to the *European Convention on Human Rights (ECHR)*. In this way, anticipating specific legislation, that would later provide a direct regulation of *privacy* as a guaranteed right in the *Union*'s legal system, the *Court* took steps to protect these fundamental rights "in practice". It did so through its jurisprudence, exactly like many individual *European* National *Courts*, on which we will shift our focus later.

In fact, another fundamental *ECJ* case, which moved in the same direction, was the 1979 *Panasonic* case, where the *Court* held that "the protection of personal data is provided by the *Community*'s legal system as one of the implicit aspects of the more extensive *right to respect for everyone's private life*"[157]. Returning to the debate on the *Nice Charter* provisions' validity, therefore, it was not a coincidence that, even in the 2003 *Philip Morris International* case, the *Court* held: "although the *Charter* does

---

[154] *Case 11-70* – "Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel" - Reference for a preliminary ruling: Verwaltungsgericht Frankfurt am Main - Germany. Judgment of the Court of 17 December 1970.
[155] *Case 4-73* – "J. Nold, Kohlen- und Baustoffgroßhandlung v. Commission of the European Communities". Judgment of the Court of 14 May 1974.
[156] *Case 44/79* – "Liselotte Hauer v. Land Rheinland-Pfalz". Reference for a preliminary ruling: Verwaltungsgericht Neustadt an der Weinstraße - Germany. Prohibition on new planting of vines. Judgment of the Court of 13 December 1979.
[157] *Case 136/79* - "National Panasonic (UK) Limited v. Commission of the European Communities". Competition: Findings of the Commission. Judgment of the Court of 26 June 1980.

not have a legally binding force, it evidences, never the less, the importance of these rights in the *Union*'s legal system"[158].

With themes and motifs often summarized, in recent times, as "soft law", the *Courts* have, in fact, come by principles which, although not expressly included in the texts of the *Community Treaties*, were already effectively part of the *European* legal system, in the name of the common constitutional traditions of the *Member States*, and of the developing International conventions, included, then, in the *Nice Charter*[159].

The "rights' compensation" carried out by the *Union's Courts*, though, no matter how exceptional, created another serious issue. In fact, admitting the "*Member States*' shared values and principles", among the *EU* Constitutional sources, contributes to doubts on competence, in case of a conflict on "the legal interpretations of rights and laws", between the *Union's Courts* and the individual *Member States*' *Courts*. In order to clear these doubts, therefore, it is necessary to briefly review the *European Courts*' competence. In this way, we can complete the picture of the *ECJ* case law, in the areas of *human rights* and *privacy*.

21. Competence of *European Court of Justice*

Issues on competence arose in the seventies, already. In fact, no matter if the 1964 *Costa v. Enel* case had cleared the primacy of *EU* law over

---

[158] *Joined Cases T-377/00, T-379/00, T-380/00, T-260/01 and T-272/01* - "Philip Morris International, Inc. and Others v. Commission of the European Communities". Decision to bring Legal Proceedings before a court in a non-Member State - Action for annulment - Concept of decision for the purposes of the fourth paragraph of Article 230 EC - Admissibility. Judgment of the Court of First Instance (Second Chamber, extended composition) of 15 January 2003.

[159] On this Pinelli C. wrote: "The adoption of a European Constitution appears to us as the time of writing the common constitutional traditions of the European peoples, including the results of the Union law experience" (*Il momento della scrittura. Contributo al dibattito sulla Costituzione europea*, Il Mulino, Bologna, 2002, page 195).

National law, both the *Italian* (*Frontini* case, 1973[160]) and the *German* (*Solange I* case, 1974[161]) *Constitutional Courts* expressly stated that "*EU* law can prevail over National law, only if it guarantees fundamental human rights" (it is important to keep in mind that these rights were not yet formally recognized in *Union* law, at the time)[162].

This doctrine, partly rectified by the *German Court* itself, in its 1986 *German Solange II* case[163], was then revived on October 12 1993, in its *Maastricht-Urteil* judgment, on the Constitutional legitimacy of the *Treaty on European Union (TEU)*[164]. Further more, if the *"Bundesverfassungsgericht"* (*German Federal Constitutional Court*) had judged it unconstitutional, it would have created serious issues to all the other *Member States*, since

---

[160] *Case n. 183* – "Frontini", Italian Constitutional Court, December 27 1973.

[161] *Solange I*, Beschluß, BVerfGE 37, 271 2 BvL 52/71, 29 May 1974.

[162] On the *Frontini* case see *The Interaction between EU and National Law in Italy. The Theory of "limits" and "counter-limits"* - Maria Dicosola ("In order to declare that the European regulations are not in conflict with the sovereignty of the State, the Constitutional Court affirmed that art. 11 Constitution does not allow limitations to the sovereignty in every case, but only in order to achieve the peace and the fairness among the Nations. Therefore, such limitations are not allowed when they are able to breach the fundamental principles of the constitutional order or the fundamental rights of the individuals."). On the *Solange I* case see *The German Constitutional Court versus the EU: self assertion in theory and submission in practice – Euro Aid and Financial Guarantees.* - Dr. Gunnar Beck ("In the Solange I case, the FCC ruled in 1974 that, in the hypothetical case of a conflict between Community law and the guarantee of fundamental rights under the German Constitution, German Constitutional Rights prevailed over any conflicting norm of EC law.").

[163] *Solange II-decision*, BVerfGE 73, 339 2 BvR 197/83, 22 October 1986. On this case see *The German Constitutional Court versus the EU: self assertion in theory and submission in practice – Euro Aid and Financial Guarantees*. - Dr. Gunnar Beck ("Solange II therefore did not affect the substance of the FCC's judgment in Solange I, namely, that the power of the national government to transfer sovereign rights extends only so far and no further than is compatible with the protection of fundamental constitutional rights and with safeguarding the basic structure of the Basic Law.").

[164] *Maastricht-Urteill*, BVerfGE 89, 155, Az: 2 BvR 2134, 2159/92, October 12 1993. On this case see *The German Constitutional Court versus the EU: self assertion in theory and submission in practice – Euro Aid and Financial Guarantees.* - Dr. Gunnar Beck ("In its long and politically charged judgment the FCC made clear that Germany's acceptance of the supremacy of Community law was limited by at least four factors: 1) the need for democratic legitimation by means of parliamentary assent (argument one), 2) the presence of a demos as the expression of the ''spiritual, social and political'' homogeneity of a people which understands itself as 'one' as a necessary source of political allegiance (argument two), 3) the constitutional guarantee of fundamental rights (argument three) and 4) the basic principles of the legal certainty and predictability as one of the constituents of the rule of law which underlie the principle of the specific transfer of limited competences (begrenzte Einzelermächtigung) to the EU (argument four).").

Germany was the last *Country* to ratify the *Treaty*, and considering the fundamental *unanimity principle*, necessary for the approval of all the *EU Treaties*.

However, the "*Bundesverfassungsgericht"*, no matter it had formally declared that it would stop creating issues on the so called "*Kompetenz-Kompetenz"* (final competence), kept its position of "dominance" on the *ECJ*, in terms of human rights-related competence, including *privacy* of course, until 1993. Anyways, after the adoption of the *Amsterdam Treaty* (1997)[165], the *Nice Charter* (2001), and the *Constitutional Draft* (2005), all the *Member States*' *Courts*, including *Germany*'s have been pragmatic enough to support the *ECJ*'s rulings, especially because of the latter's gradually increasing protectionism of human rights.

22. Monistic or Dualistic Approach

Since its establishment, the *ECJ* has always adopted a "monistic" approach to represent the relationship between the *Union*'s legal system and the legal system of the *Member States*, differently from many National *Courts*.

In fact, in its landmark 1984 *Granital* judgment, for example, the "*Corte Costituzionale"* (*Italian Constitutional Court*) expressly stated: "the *Court of Justice (ECJ)* considers, it is true, the source of the *Community* legislation and that of the *State* (*Italy*) as integrated into one single system, and therefore moves from different premises than those reflected in the jurisprudence of this *Court"* (the *Italian* one).[166] Therefore, from the *Italian Court*'s "dualistic" point of view, it has been historically very difficult to evaluate the

[165] "The Amsterdam Treaty, officially the Treaty of Amsterdam amending the Treaty of the European Union, the Treaties establishing the European Communities and certain related acts, was signed on 2 October 1997, and entered into force on 1 May 1999; it made substantial changes to the Treaty of Maastricht, which had been signed in 1992" ("Amsterdam Treaty", *Wikipedia*).
[166] *Case 170/84* – "Granital", Italian Constitutional Court, June 8 1984.

Constitutionality of some *Italian Parliament*'s provisions in accordance with *EU* law.

The "*Bundesverfassungsgericht*" "monistic" approach, instead, forced *Germany* to amend its 1949 *Constitution*, for an evident violation of human rights, following the 1998 *Kreil* case[167]. In this case, commenced in 1998, *Tanja Kreil* argued the Constitutionality of the ban for women to be enrolled in the army. Further more, following the acceptance of the application by the *ECJ*, the *European Council* also adopted a *Directive*, which "precludes the application of National standards, such as those of *German* law, which generally exclude women from military posts involving the use of arms"[168]. On the basis of this judgment, as already mentioned, the *Federal Republic of Germany* had to, therefore, amend *Article 12a(4)* of its *Constitution*[169].

However, whether if it is reached through a "monistic" or a "dualistic" approach, what matters in the end is the substantial legal convergence between the *EU's* and the *Member States'* laws. This should of course be the reached goal, given the original common desire to create a single *Union*'s legal system, aimed at the protection of fundamental human rights (specifically, for our analysis, for the protection of *privacy*).

Given the general terms of *Article 234* of the *Treaty*[170], though, it is quite normal to have conflicts on jurisdiction between the *ECJ* and the *Courts*

---

[167] *Case C-285/98* - "Tanja Kreil v Bundesrepublik Deutschland". Reference for a preliminary ruling: Verwaltungsgericht Hannover - Germany. Equal treatment for men and women - Limitation of access by women to military posts in the Bundeswehr. Judgment of the Court of 11 January 2000.

[168] *Council Directive 2000/78/EC* - "Establishing a general framework for equal treatment in employment and occupation", November 27 2000.

[169] *Article 12a [Compulsory military and alternative civilian service]* (4) "If, during a state of defense, the need for civilian services in the civilian health system or in stationary military hospitals cannot be met on a voluntary basis, women between the age of eighteen and fifty-five may be called upon to render such services by or pursuant to a law. Under no circumstances may they be required to render service involving the use of arms". (*Basic Law for the Federal Republic of Germany*).

[170] *Article 234* - Part Five: "Institutions of the Community" - Title I: "Provisions governing the institutions" - Chapter 1: "The institutions" - Section 4: "The Court of Justice", *Treaty establishing the*

of the *Member States*. Beyond this, given the *Article*'s final provision: "Where any such question is raised in a case pending before a court or tribunal of a *Member State* against whose decisions there is no judicial remedy under National law, that *Court* or *Tribunal* shall bring the matter before the *Court of Justice*"[171], it is quite clear that the *ECJ*'s competence is greater, and should always prevail.

23. Constitutionally-Relevant *Treaty*-Provisions

Having analyzed the *Charter*'s provisions, and the jurisprudence of the *ECJ*, it is time to look at the *Treaties*' provisions, in order to complete the picture of *EU* law's Constitutional sources. The reason why typical instruments of International law, such as the *Treaties*, hold the rank of Constitutional law in the *European Union*'s legal system depends on the principle of the *acquis communautaire*, which can be interpreted as the "consolidated legal heritage" of the *Union*.

In fact, while in common International law, the parties are not usually bound by prior arrangements, when discussing new Treaties, in *Union* law instead, the negotiations that lead to any new agreement move from the *acquis communautaire,* consolidated so far. An example of this trend was the *Les Verts* case, in 1986, in which the judges of the *Court of Justice* referred several times to the *EU Treaties* as " the fundamental Constitutional Charter"[172].

European Community ("Nice consolidated version", *www.eur-lex.europa.eu*). Now substituted by *Article 267 TFEU* (Draws on Article 234 TEC. Extends preliminary rulings jurisdiction to TEU and to acts of EU bodies, offices and agencies. Adds urgency requirement in cases involving persons in custody).

[171] Id.

[172] *Case 294/83* - "Parti écologiste "Les Verts" v. European Parliament". Action for annulment - Information campaign for the elections to the European Parliament. Judgment of the Court of April 23 1986.

Regarding the most Constitutionally relevant provisions of the *Treaties*, in terms of *privacy* protection, it is important to start from *Article 6* of the *TEU*[173]. While the *First Section* solemnly affirms that the *European Union* "is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the *Member States*"[174], the *Second Section* repeats what was said by the jurisprudence of the *Court of Justice*. In fact, it proclaims that the *Union* is bound to "respect fundamental rights, as guaranteed by the *European Convention of Human Rights* and as a result from the common Constitutional traditions of the *Member States*, as general principles of *Community* law"[175].

Other important Constitutional provisions were definitely *Articles 95, 230* and *300* of the *EC Treaty*, despite essentially providing rules of procedure[176]. As explained by the *Judges* of the *Court of Justice,* in a 2001 opinion, "the choice of the appropriate legal basis has Constitutional significance. As the *Community* has only conferred powers, it is linked with the provisions of the *Treaty*, which enables it to adopt the appropriate measures "[177].

Further more, another Constitutionally important *privacy*-related provision was *Article 286 (1)* of the *EC Treaty*, which stated that "with effect from 1 January 1999, *Community* acts on the protection of personal data as well as the free movement of such data shall apply to the Institutions and

---

[173] *Article 6 (ex article 6 TEU)* - Title I "Common Provisions", *Consolidated Version of the Treaty on European Union*.
[174] Id.
[175] Id.
[176] *Articles 95, 230* and *300* - *EC Treaty*, now respectively substituted by *TFEU Articles: 114* (In substance the same as Article 95 TEC), *263* (Extends scope of jurisdiction to review legality of acts covering EU institutions, bodies, offices and agencies), and *218* (Draws on Article 300 TEC and Articles 24 and 38 TEU, but reorganizes, amends and supplements them. A special procedure is included regarding EU accession to the European Convention on Human Rights).
[177] *ECJ Opinion 2/00*, on *Article 300 (6) TEC*, 2001, § 5.

Agencies established by this *Treaty* or on its basis.[178]" This provision also led to the creation of the *European Data Protection Supervisor*[179].

However *Article 286* of the *TEC* was later replaced and expanded by the *Article 16* of the *TFEU*, in 2009[180]. Finally, after analyzing the Constitutional sources of *EU* law, it is time to shift our focus to the ordinary *EU* law in the *privacy* area, starting from the so-called *"Data Protection Directive" (95/46/EC)*[181].

24. EU Ordinary *Privacy* Law and *Directive 95/46/EC*

The most important ordinary law of the *Union*, in the *privacy* area, is definitely *Directive 95/46/EC*, "On the protection of individuals with regard to the processing of personal data and on the free movement of such data"[182]. The *European Parliament* and *Council* have approved the *"Data Protection Directive"* on October 24 1995, on the basis of *Article 100(a)* of the *EC Treaty* (now *Article 114 TFEU*)[183]. This *Directive* was inserted in the wider context of *Title VI* of the *TEU*, regarding police and judicial cooperation in criminal

---

[178] *Article 286 - EC Treaty,* now replaced by *Article 16* of the *Treaty on the Functioning of the European Union (TFEU).*

[179] "Privacy & Data Protection" ADVISORY, *Covington & Burling LLP*, November 23, 2009.

[180] *Article 16 (ex Article 286 TEC)* – "1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union", *Consolidated version of the Treaty on the Functioning of the European Union*.

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

[182] Id.

[183] "In article 95 (ex 100A, since Lisbon art. 114 TFEU), governing the internal market, the possibilities are set out for more stringent national requirements to be implemented, despite the European harmonization rules". (Douma W.T. - "European Environmental Law after Lisbon: an introduction", *Asser Institute, Center for International & European Law*).

matters, with the agreements signed on June 14 1985, in *Schengen* (later incorporated in the homologous *Convention*, on June 19 1990[184]).

The idea that inspired the *Directive* was expressed clearly in its *Preamble*: "the establishment and functioning of an internal market (...) require not only that personal data can move freely from one *Member State* to another, but also that the rights of individuals' are protected"[185]. In general terms, the goal for the *EU Member States*, as set out in *Article 1* of the *Directive*, is to "protect the fundamental rights and freedoms of individuals, and in particular their right to *privacy* in regards to personal data processing"[186].

At the operational level, therefore, *Paragraph 8* of the *Preliminary Considerations* states: "in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all *Member States*"[187]. Consequently, the implementation of the *Directive* in each *Member State*, first, and the application of the judicial measures provided by *Union* law, afterwards, can effectively guarantee that "equivalent" treatment.

However, in order to analyze this *Directive* properly, it is important to deal separately with five key points. These, respectively, consist in: the definition of "personal data" and of "data processing", the principles of

---

[184] *The Schengen acquis* – "Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders".
[185] *Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[186] *Article 1, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[187] *Section 8 of the Preliminary Considerations, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

legitimacy underlying data processing itself, the special regime for the so-called "sensitive data", the exceptions and limitations provided for cases related to *National security* and, finally, the area of operability of these measures.

In fact, in contrast with the *American* sectorial approach, analyzed in *Chapter I*, the objective of the *European* provisions is not only to guarantee a minimum level of "personal" protection, but also to ensure "general" *privacy* protection. This goal was confirmed fairly recently by the *European Court of Justice*, in the 2003 *Lindqvist* case[188]. Therefore, in order to balance the free movement of personal data with the protection of *privacy*, the point was to establish a set of obligations for those entities that process data, and to ensure all individuals three rights in particular: the free access to data regarding them, the ability to modify and delete such information when appropriate, and, finally, to refuse in certain circumstances that their data can be processed. But let us now analyze the "key points" of *Directive 95/46/EC*.

First of all, the *Data Protection Directive* defines "personal data" in *Article 2, Section a* as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[189]. "Data

---

[188] *Case C-101/01* – "Criminal proceedings against Bodil Lindqvist". Reference for a preliminary ruling: Göta hovrätt - Sweden. Directive 95/46/EC - Scope - Publication of personal data on the internet - Place of publication - Definition of transfer of personal data to third countries - Freedom of expression - Compatibility with Directive 95/46 of greater protection for personal data under the national legislation of a Member State. Judgment of the Court of November 6 2003.

[189] *Article 2, Section a, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

processing", instead, is defined in *Article 2, Section b* as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"[190].

By reading further the *Directive*, also the "principles of legitimacy underlying data processing" become clearer. In fact, as set forth in *Article 6*, regarding the "quality" of the data, the latter must be "processed fairly and lawfully", and "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". Furthermore, the data must be "accurate and, where necessary, kept up to date", "and not excessive in relation to the purposes for which they are collected and/or further processed". [191].

The conditions for the data to be lawfully processed, in accordance with the quality standards laid down in *Article 6* of the *Directive*, are established, instead, by *Article 7*. In fact, *Article 7,* on one hand, provides, in *Section a,* that personal data may be processed only if "the data subject has unambiguously given his consent", as a first hypothesis of legitimacy. On the other hand, it lists five additional cases in which the data can be processed, beyond the subject's consensus[192].

---

[190] *Article 2, Section b, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[191] *Article 6, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[192] *Article 7, Section a, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

In particular, *Article 7* provides that "*Member States* shall provide that personal data may be processed" also if "necessary": "for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (*b*), "for compliance with a legal obligation to which the controller is subject" (*c*), "in order to protect the vital interests of the data subject" (*d*), "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" (*e*), and "for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed" (*f*)[193].

Further more, especially in case of "unambiguous consensus" (*Article 7, Section a*), *Article 10* of the *Data Protection Directive* provides that the subject must receive the necessary information to understand the purposes for which his data are collected, and to know who is responsible for processing his data, the recipients or categories of recipients to whom the his data are processed, and if answering the questions is mandatory or not. In case it is, the applicant must then be aware of the consequences for the possible non-response and, in any case, whether or not there is a right of access and correction, in regards to all the data relating to him[194].

Article 8 of the *Directive*, instead, provides a special regime for the case in which the processed data regard the health or sexual behavior of people, their political views, ethnic origin, etc. Therefore, after analyzing the

---

[193] *Article 7, Sections b-f, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

[194] *Article 10, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

"quality" and the "legitimacy" of the processed data, we must now look at the so-called "sensitive data"[195]. In fact, *Paragraph 1* establishes that "*Member States* shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life"[196].

The following *Paragraphs* of *Article 8*, however, introduce a significant number of exemptions and exceptions, ranging from labor relations to scientific research, and from the processing of medical data to judicial records and the register of criminal convictions, for which the *Member States*, unless there is a notification to the *Commission*, are granted a wide range of action. For example, it is up to the *Member States* to determine whether and under what conditions the national identification numbers can be processed, as in the case of identity cards. Further more, when an individual authorizes the release of data relating to his origin, health and sex life, political opinions, religious beliefs or trade union membership, it is always up to the *State* to establish, by law, whether the given consent is sufficient or not[197].

These *Member States*' measures, however discretional, have an impact on the safe treatment of the data, and therefore have to provide "a level of *security* appropriate to the risks represented by the processing and the nature of the data to be protected", in accordance with *Article 17* of the

---

[195] *Article 8, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[196] *Article 8, Paragraph 1, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[197] *Article 8, Paragraph 2, Section a, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

Directive[198]. *States* can thus establish that "processing of data relating to offences, criminal convictions or *security* measures may be carried out only under the control of official Authority", as in the case of "data relating to administrative sanctions or judgments in civil cases"(*Article 8, Paragraph 5*)[199].

Member States may also, "for reasons of substantial public interest, lay down exemptions in addition to those laid down in *Paragraph 2* either by National law or by decision of the *Supervisory Authority*" (*Article 8, Paragraph 4*)[200]. Therefore, this brings us back to the theme of *National security*, a key element for our analysis, which is directly addressed in *Article 13* of the *Directive*[201].

25. National Security in *Directive 95/46/EC*

National security issues arise both from the technical requirements of data protection, and from the general risks of information flows. In some cases, therefore, most of the mentioned rights and obligations have to surrender before the demands of the *State*'s *security*.

Among these cases, *Paragraph 1 of Article 13* lists 7 main ones: "state *security*" itself (*Section a*), "defense" (*Section b*), "public safety" (*Section c*), the case of "criminal offenses or of breaches of ethics for regulated

---

[198] *Article 17, Paragraph 1, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[199] *Article 8, Paragraph 5, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[200] *Article 8, Paragraph 4, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[201] *Article 13, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

professions" (*Section d*), "an important economic or financial interest of a *Member State* or the *European Union*, including monetary, budgetary and taxation" (*Section e*), various tasks related to the exercise of public authority referred to in the previous three *Sections* of the *Article* (*Section f*), and, finally, the "protection of the data subject or the rights and freedoms of others" (*Section g*)[202].

The range of action of the *Directive* is further defined by the provision contained in *Paragraph 2* of *Article 3*, which refers to "the activities of the *State* in areas of Criminal law", mentioned before. In fact, the applicability of the *Directive* is expressly excluded "in the course of an activity which falls outside the scope of *Community* law, such as those provided for by *Titles V* and *VI* of the *Treaty on European Union* and in any case to processing operations concerning public *security*, defense, *State security* (including the economic well-being of the *State* when the processing operation regards *State security* matters)"[203].

In light of these provisions, which partially trace the *boundaries* between the rights to *individual privacy* and to *National security*, in the *European Union*, we must now analyze one of the most important news of this *Directive*, i.e., the establishment of *Authorities* in the field of *privacy*[204].

---

[202] *Article 13, Paragraph 1, Sections a–g, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[203] *Article 3, Paragraph 2, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[204] *Article 28, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

26. Supervisory Authorities

In the end, it would be useless to proclaim “the rights of access, modification or deletion relating to personal data, with the obligation to prosecute them lawfully and fairly, given the informed consent of those concerned (when necessary), with the safety measures required by law”, if, in practice, all of this would not be strictly supervised by *Authorities*.

In order to accomplish this goal, beyond the ordinary judicial protection, the *EU Directive* establishes that the *Supervisory Authorities* should have investigative powers, the powers to intervene and also to promote a legal action, in case the general provisions for the protection of *privacy* are violated (*Article 28, Paragraph 3*)[205]. Any person concerned, on the other hand, may submit to the *Supervisory Authorities* a complaint "concerning the protection of his rights and freedoms in regard to the processing of personal data" (*Article 28, Paragraph 4*)[206].

Further more, independently from the *Member States*' National provisions, the *Supervising Authorities* may also order "the blocking, erasure or destruction of data", impose "a temporary or definitive ban on processing", warn or admonish the controller, or can refer "the matter to National *Parliaments* or other political institutions "(*Article 28, Paragraphs 3 and 5*)[207].

---

[205] *Article 28, Paragraph 3, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[206] *Article 28, Paragraph 4, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.
[207] *Article 28, Paragraphs 3 and 5, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995.

However, the introduction of *Supervising Authorities* was a novelty in civil law legal systems, such as the *Italian* and the *French*[208]. It is therefore quite useful, for our analysis, to see the different ways this fundamental *Directive* has been implemented throughout some of the main *EU Member States*. In this way, we can understand further the peculiarity of the "non-federal" *European Union*, a legal system that encloses many others. In fact, in the *privacy* area, as in many others, the *EU* legal system has left a wide range of discretion to its *Member States*, in order to obtain the results required by the *Data Protection Directive*, and without prejudice to the essential purpose of achieving a common specific goal.

27. Implementation of *Directive 95/46/EC* in *Italy*

Directive 95/46/EC was implemented in *Italy* through *Law 675/1996* in 1996[209]. This *Law*[210], though, was later replaced by *Legislative Decree*

---

[208] U. Pagallo points out that from a general theory of law point of view, one of the major issues raised by the introduction of Authorities in Civil law systems, such as the Italian, depends on its hard insertion within the canonical division of the three powers of State. While in fact, Common law systems, that provide a check and balances mechanism, focus on the dualism between Government bodies and the Courts, therefore, the powers of the Authorities can be easily incorporated within the sphere of "iurisdictio". In Civil law systems, instead, these powers end up not to be attributed entirely to the executive branch nor to the judiciary branch. On the other hand, with respect to the (not only) French administrative tradition, which subordinates, ultimately, the executive bodies to the political power, Authorities have the further peculiarity of being independent (*La Tutela della Privacy Negli Stati Uniti D'America e in Europa*, Giuffrè Editore, 2008, page 133).

[209] To comply with the *Schengen Agreement* and to implement the *Directive 95/46/EC*, *Law 675/1996*, on the "Protection of persons and other subjects regarding the processing of personal data", was enacted on December 31, 1996, and came into force in May 1997.

[210] Rodotà S. points out that Law 675/1996, however, was not greeted with particular enthusiasm by the Italian public. "The judgments which preceded the entry into force of the legislation, in fact, had identified the right to privacy as a right of the elite, of those who were privileged, under the eyes of the spotlight, and who claimed a right to sit on their own: actors, musicians, politicians, famous people . The right to privacy, in Italy, was in fact intended almost as a superfluous law for ordinary people, such as the upper middle class' right claimed by Warren and Brandeis. Actually, it seemed to reflect a suspicious need, able to break the bonds of social solidarity that had been so relevant in our country. We wondered why ordinary citizens might feel the need to isolate themselves, to be alone. Not even the political class considered it much, believing that it was a luxury right, and not relevant for the public opinion" (*Intervista su privacy e libertà*, a cura di Paolo Conti, Editori Laterza, Roma-Bari, 2005, page 25).

196/2003 in 2003[211], entitled "*Code of Personal Data Protection*", and usually referred to as the "*Privacy Code*"[212].

Legislative Decree 196/2003 entered into force on January 1 2004. The purposes of this *Legislative Decree* were the recognition of the right of individuals over their personal data and, consequently, the discipline of the various "data treatment" operations: collection, processing, comparison, deletion, modification, disclosure and dissemination[213]. However, several *MP*'s referrals, regarding the application of *minimum-security measures*, have delayed the full implementation of this *Legislative Decree*, until March 31 2006.

The previous *Law 675/1996* regarded mostly the big companies, from both a physical and an organizational point of view, which were interested in data treatment [214]. However, the intensive use of Internet and its applications, and the awareness of the right to personal data protection, in a continuously growing population, has forced the *Italian Legislator* to draft a more appropriate legislation. *Legislative Decree 196/2003*, therefore, substituted *Law 675/1996*, and all the related regulations[215].

---

[211] The code "on the protection of personal data", or legislative decree (act having the force of law) n. 196 of the Italian Republic, also commonly referred to as the "Privacy Code", was issued on June 30 2003, and entered into force on January 1 2004.

[212] Russo S. – Sciuto A. - "La Protezione dei Dati Personali nella Normativa UE e in Italia", *Habeas Data e Informatica*, Giuffrè Editore, 2011, page 83.

[213] Id.

[214] *Legge n. 675 del 31 dicembre 1996* - "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", *Garante Per La Protezione Dei Dati Personali* (*www.garanteprivacy.it*).

[215] *Legge 676/1996, 31 dicembre 1996*: Legge delega; *D.L. n.135, 11 maggio 1999*: "Disposizioni integrative sul trattamento di dati sensibili da parte dei soggetti pubblici"; *D.L. n.281, 30 luglio 1999*: "Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica"; *D.L. n.282, 30 luglio 1999*: "Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario"; *D.P.R. n.318, 28 luglio 1999*: "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali"; Provvedimento del Garante per la protezione dei dati personali, n.1/P/2000: "Individuazione dei dati sensibili da parte dei soggetti pubblici".

The *Italian Privacy Code* is divided into three parts. The first, entitled "General provisions" and including *Articles 1 to 45*, contains the main principles of *privacy*, its rights and how to exercise them, and also the consequent duties in terms of personal data treatment[216]. *Article 1* of *Decree 196/2003*, for example, recognizes the absolute right of individuals on their own data: "Everyone has the right to the protection of personal data concerning him"[217]. The second part of the *Privacy Code*, instead, is entitled "Provisions relating to specific sectors", and comprises *Articles 46 to 140*. It concerns only the treatments carried out in specific areas: judiciary, police, defense and state *security*, public administration, health, education, and so on[218].

Finally, since the respect of all of the *Italian* laws and regulations on *privacy* are supervised by the "*Garante della Privacy*" (*Italian Privacy Authority*)[219], the third part of the *Decree*, entitled "Protection of the person concerned and sanctions", and including *Articles 141 to 186*, provides the rules for this *Authority*'s controls. It specifically regulates "the administrative and legal protections of the *Garante*", "the procedures to file a report, a complaint or an appeal to the *Garante*", "the prerogatives of the *Garante*, of its office and organs of investigation", "the penalties for administrative violations and criminal offenses", "the provisions for amendment and abrogation of previous legislation", and also "the transitional and final provisions"[220].

---

[216] *Decreto Legislativo 30 giugno 2003, n. 196* - "Codice in Materia Di Protezione Dei Dati Personali", *Garante Per La Protezione Dei Dati Personali*.
[217] Id.
[218] Id.
[219] "L'Autorità", (*www.garanteprivacy.it*).
[220] *Decreto Legislativo 30 giugno 2003, n. 196* - "Codice in Materia Di Protezione Dei Dati Personali", *Garante Per La Protezione Dei Dati Personali*.

Further more, several *Annexes* complete the *Privacy Code*[221]. However, we can say that the overall *Italian* discipline on the protection of personal data was not changed much by the *Privacy Code*, since the purpose of this *Decree* consisted, basically, in reuniting the entire set of rules, already existing in *Law 675/1996*, and in the other *Italian* complementary *privacy* laws[222].

28. Implementation of *Directive 95/46/EC* in *France*

EU Directive 95/46 was implemented in *France* only in 2004, after the approval by its *Constitutional Council* of the new *Law on Data Protection* ("*LOI n. 801/2004"*)[223]. Compared to the previous *Law*, which dates back to 1978 ("*LOI 78/17, relative à l'informatique, aux fichiers et aux libertés"*)[224], the new *Law* increased the sanctioning powers of the *French Data Protection Authority* ("*Commission Nationale de l'Informatique et des Libertés" or "CNIL"*)[225].

Further more, *Law n. 801/2004* eliminated the notification requirement for those who appoint a "reference person for data protection" and disposed the obligation to submit a preliminary assessment by the *CNIL*,

---

[221] Id.

[222] *Legge 676/1996, 31 dicembre 1996*: Legge delega; *D.L. n.135, 11 maggio 1999*: "Disposizioni integrative sul trattamento di dati sensibili da parte dei soggetti pubblici"; *D.L. n.281, 30 luglio 1999*: "Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica"; *D.L. n.282, 30 luglio 1999*: "Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario"; *D.P.R. n.318, 28 luglio 1999*: "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali"; Provvedimento del Garante per la protezione dei dati personali, n.1/P/2000: "Individuazione dei dati sensibili da parte dei soggetti pubblici".

[223] *LOI n° 2004-801 du 6 août 2004* - "relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la *LOI n° 78-17 du 6 janvier 1978* - "relative à l'informatique, aux fichiers et aux libertés".

[224] *LOI n° 78-17 du 6 janvier 1978* - "relative à l'informatique, aux fichiers et aux libertés".

[225] *LOI n° 2004-801 du 6 août 2004* - "relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la *LOI n° 78-17 du 6 janvier 1978* - "relative à l'informatique, aux fichiers et aux libertés".

on any treatment involving the use of biometrics[226]. In fact, this was the result of a long and tormented legislative process, which lasted over two years and started much later than the implementation deadline required by the *EU Directive* (October 24 1998).

Law n. 801/2004 also regulated personal information treatment by *Government* Agencies and in the private sector, introducing compulsory registrations and authorization requests, in order to process personal data, in many cases involving the public administration, and in the health sector. Individuals must be informed in advance about the purposes, the methods of collection, and the storage of personal data concerning them, and may object to their treatment, at any time. They also have the right to request access, updating, and in some cases the cancellation of those data. Finally, *Law n. 801/2004* provided both administrative and criminal sanctions for treatments in violation of the *Law*[227].

As already mentioned, the *French Authority for the Protection of Personal Data* is the *Commission Nationale de l'Informatique et des Libertés*, an independent *Government Agency*, which monitors the compliance to the *Law on Data Protection* and other related legislation[228]. The *Commission* investigates complaints, issues prescriptions and regulations, conducts audits, studies and issues periodic reports, and is responsible for managing the *National Register of Personal Data*.

On the basis of the *2004 Amendment* to the *Law on Data Protection*, the *CNIL* has also investigative duties, on the processing of data, and may issue

---

[226] Id.
[227] Id.
[228] *CNIL - Commission Nationale de l'Informatique et des Libertés* (*www.cnil.fr*).

regulations and impose fines, up to 150,000 euros[229]. In 2006, for example, the *CNIL* sanctioned the banking group "*Crédit Lyonnais"* with an administrative fine of 45,000 euros, since it had violated the *right of access* of its clients to their personal data[230]. Further more, the *French Criminal Code* has tightened the sanctions in case of a breach of *Law n. 801/2004* (up to 5 years imprisonment and a fines up to 300,000 euros, depending on the case).

Beyond this, the *Commission* can dispose other measures, or regulatory sanctions, in cases involving the use of biometric data (especially in identification documents), direct marketing, spamming, and electronic surveillance. The *Commission* does not have an official e-mail address; therefore, all initial contacts should be made exclusively by regular mail, since they are more *privacy*-efficient. Finally, *Law n. 801/2004* provided *legal persons' criminal liability*, with the possibility of declaring their "legal interdiction"[231].

29. Implementation of *Directive 95/46/EC* in *Germany*

To start our analysis on *Germany*, me must say that its *Law* on *Personal Data Protection* has always been among the most restrictive in the entire *European Union*. Actually, the first law in the world in the field of data protection was approved in *Germany*, specifically in the region of *Hessen*, in 1970. This *Law* was followed, in 1977, by the *Decree on the Federal Data Protection* ("*Bundesdatenschutzgesetz"* or *"BDSG"*), and then amended, in

---

[229] *LOI n° 2004-801 du 6 août 2004* - "relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la *LOI n° 78-17 du 6 janvier 1978* - "relative à l'informatique, aux fichiers et aux libertés".

[230] *Délibération n° 2006-174 du 28 juin 2006* – "prononçant une sanction pécuniaire à l'encontre du Crédit Lyonnais (LCL) " (*www.cnil.fr*).

[231] *LOI n° 2004-801 du 6 août 2004* - "relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la *LOI n° 78-17 du 6 janvier 1978* - "relative à l'informatique, aux fichiers et aux libertés".

1990, in 1994, and in 1997[232]. However, its first complete revision was published in 2003, and the latest revisions of *German privacy* laws are the *Federal Laws* of July 29 2009 and of August 14 2009[233].

The *BDSG* protects the right of individuals in regards to the processing of their personal data. It includes all the operations of collection, processing and use of personal data, automatic or manual, by *Federal Authorities*, *Regional Governments* and private organizations, for both commercial and professional purposes[234]. The main provisions of the *BDSG* regard "transfer of personal data abroad", "video surveillance", "direct marketing", "anonymous communications", "use of pseudonyms", "smart cards", and the "collection and storage of personal data of sensitive nature"[235]. Interested parties have the right to request access, modification or deletion of personal data, and to oppose their treatment, in certain circumstances[236].

Further more, managers of personal data, in both the public and the private sectors, who have more than nine appointees to the treatment, must appoint one of them "responsible for the internal *security* of the data", or are required to record all the automated processes at the *Federal Commissioner for data Protection ("BFDI")*[237]. Each "*Lander*" (*Region*) also has its specific

---

[232] "In the year 1970 the federal state of Hessen passed the first national data protection law, which was also the first data protection law in the world. In 1971 the first draft bill was submitted for a federal data protection act. Eight years later, on 1.1.1979, the first federal data protection act came into force. In the following years in which the BDSG was taking shape in practice, a technical development took place in the data processing as the computer both at work and in the private sector became increasingly important"("Bundesdatenschutzgesetz", *Wikipedia*).

[233] *Federal Data Protection Act (BDSG)* - In the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814).

[234] Id.

[235] Id.

[236] Id.

[237] *German Data Protection Authority*, (*www.bfdi.bund.de*).

laws on data protection, regarding treatments carried out by its management bodies, and in its private activities[238].

The *Federal Commissioner for Data Protection and Freedom of Information ("Bundesbeauftragter für den Datenschutz" or "BFDI")* is an independent *Federal Agency*, responsible for monitoring the application of the *Decree on the Federal Data Protection (BDSG)* and the *Federal Decree on Freedom of Information*. The *BFDI* coordinates and monitors the activities of public bodies of the Federation, in relation to the provisions of the *BDSG*. Beyond this, it manages the *Federal Register of Personal Data*, investigates complaints and reports from interested parties, provides recommendations to the *Parliament* and *Government Bodies*, and publishes a biennial report on its activities, and on the implementation of the *Law*.

Moreover, the *President* of the *BFDI* is an official of the *German Chancellery*[239]. For this reason, the *European Union* started an infringement proceeding against *Germany* for "insufficient independence of their *Authority for Data Protection*", in July 2005[240].

However, each *Lander* has a local *Commissioner for Data Protection*, with supervising powers over the activities of the public and the private sectors. In some *Landers*, the *Commissioner* deals exclusively with the control over the activities of the public sector, and there is a *Surveillance Authority* for the control of those in the private sector. The *Commissioner of Berlin*

---

[238] *German Privacy Authorities Website*, "Virtuelles Datenschutzbüro" (*www.datenschutz.de*).
[239] *German Data Protection Authority*, (*www.bfdi.bund.de*).
[240] *Case C-518/07* - "European Commission v Federal Republic of Germany". Failure of a Member State to fulfill obligations - Directive 95/46/EC - "Protection of individuals with regard to the processing of personal data and the free movement of such data" - Article 28(1) - National supervisory authorities - Independence - Administrative scrutiny of those authorities. Judgment of the Court (Grand Chamber) of 9 March 2010.

coordinates all *Supervisory Authorities* in *Germany*[241]. Beyond this, since the *German Constitution* guarantees total autonomy to the churches[242], these have their own *Authorities for the Protection of Personal Data*, in accordance with the *BDSG*. Finally, on the basis of *Article 41* of the *BDSG*, *"Autonomous Authorities* provide the control over broadcasters"[243].

30. Implementation of *Directive 95/46/EC* in the *UK*

In the *United Kingdom*, instead, *Directive 1995/46/EC* was implemented by the *Parliament*, through the 1998 *Data Protection Act*, at first[244], and through the 2000 *Freedom of Information Act*, afterwards[245].

These *Acts*, which came fully into force only in 2005, applied to personal data processing, in both the public and the private sectors. They introduced eight basic principles for data protection, in accordance to the *European Directive*, setting limits to the use of personal information in relation to the purposes of treatment, adequate measures of *security* procedures for "access to" and "correction of" data, and the obligation to register data managers at the *British National Authority for Data Protection* ("*Information Commissioner Office"*) [246]. These *Acts*' last amendments came into force on November 12 2009[247].

However, the *Data Protection Act* and the *Freedom of Information Act* have been strongly criticized by the *Commissioner* and by the judicial bodies,

---

[241] *Commissioner of Berlin* Website – "Berliner Beauftragter für Datenschutz und Informationsfreiheit" (*www.datenschutz-berlin.de*).
[242] *Basic Law for the Federal Republic of Germany*.
[243] *Article 41*, *Federal Data Protection Act (BDSG)* - In the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814).
[244] *Data Protection Act 1998*.
[245] *Freedom of Information Act 2000*.
[246] "Freedom of Information and Data Protection", *Companies House* (*www.companieshouse.gov.uk*).
[247] Id.

for their complexity and for their lack of clarity and effectiveness, in protecting the *privacy* of the parties concerned.

Overall, the culture of *security* and data protection is still insufficient in the *UK*, since there are frequent cases of "leaks" of personal information from *Government* databases, both fortuitous and intentional. In 2006, the *Information Commissioner Office* has published two reports, demonstrating a worrying increase of illegal trade, of personal data and information, between the police and the private detective agencies[248].

For this reason, on October 29 2009, the *European Commission* launched the second stage of an infringement procedure of the *EU Directive on Data Protection* against the *UK*, because it did not provide an independent *Authority* for the interception of communications' control. Further more, the *British Regulation of Investigatory Powers Act 2000 (RIPA)*, which lays down the rules on wiretapping communications, enabled to intercept even those, who simply had "reasonable grounds to believe" that consent has been granted. Finally, the *UK Law* punished only the "intentional" interceptions[249].

The *Information Commissioner's Office* is an independent *Government* agency, responsible for managing the *National Data Register*, in order to comply with the *Data Protection Act*, the *Freedom of Information Act*, and the *Electronic Communication Regulations*[250]. It is important to point out that more than 25 percent of the cases handled by the *Commissioner*, over the years, have regarded the latter *Regulations*. The *Information Commissioner's Office* has limited powers and no ability to provide sanctions; it can only

---

[248] "What price privacy? The unlawful trade in confidential personal information", Presented by the *Information Commissioner* to *Parliament* pursuant to *Section 52(2) of the Data Protection Act 1998*, Ordered by the *House of Commons* to be printed 10 May 2006 (*www.ico.org.uk*).
[249] "The European Commission refers UK to Court over privacy and personal data protection", *European Commission*, *United Kingdom*, Press Room Press releases, 2010 (*www.ec.europa.eu*).
[250] *Information Commissioner's Office* (*www.ico.org.uk*).

report suspected violations of the *privacy* statements, and the names of the alleged perpetrators, to the competent judicial authorities[251]. Further more, reporting the perpetrations of the 2005 *Employment Practices Data Protection Code*, relating to *privacy* in the workplace is among the main activities of the *Information Commissioner's Office* [252].

In *Scotland*, instead, there is the *Scottish information Commissioner*, who is responsible for enforcing the laws, promoting freedom of information, and reporting violations of the *Act on Data Protection* to the judicial authorities[253]. The *Scottish Commissioner* is mainly interested in the *Freedom of Information (Scotland) Act*, of 2002[254], and in the *Environmental Information (Scotland) Regulations*, of 2004[255], both of which came into force on January 1, 2005. These laws concern mainly the individuals' *right of access* to their information, which is held by more than 10,000 public bodies, in *Scotland*[256].

31. Implementation of *Directive 95/46/EC* in *Spain*

In *Spain*, the *EU Directive on Privacy* was implemented on December 13 1999, through *Organic Law 15/1999 on Personal Data Protection* ("*Ley Orgánica 15/1999 de Protección de Datos de Caracter Personal*"), which replaced the previous *Law* of *1992*[257]. In fact, the *Ley Orgánica 15/1999* established the right of citizens, in both the public and the private sectors, to know what data is contained in electronic files, and to have those data

---

[251] Id.
[252] *The Employment Practices Code*, "Data Protection", *ICO*.
[253] *Scottish information Commissioner* (*www.itspublicknowledge.info*).
[254] *Freedom of Information (Scotland) Act 2002*.
[255] *The Environmental Information (Scotland) Regulations 2004*.
[256] "Scottish Public Authorities", *Scottish information Commissioner* (*www.itspublicknowledge.info*).
[257] *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal* (Texto consolidado a fecha 5 de marzo de 2011).

corrected or deleted, if they are incorrect or false. Moreover, it provided that disclosure of data to third parties could only occur with the consent of the persons concerned, except in direct marketing, where consent should not be required, but could be denied later on[258].

In June 1999, instead, *Spain* had issued the *Royal Decree 994/1999 "on security measures for computer files containing personal data"*. By this *Decree*, data managers have been obliged to introduce the information related to their databases in the *Register of Information Archives*, whether containing personal or sensitive data[259]. Later on, specifically on June 11 2007, *Spain* also issued the *Royal Decree 1720/2007*, in order to amend *Law 15/1999*, and for it to fully incorporate the new *European Union Directives*[260].

The *Spanish Agency for Data Protection ("Agencia Española de Protección de Datos" or "AEPD")* enforces the law and the regulations on data protection, manages the *Databases Register*, and can investigate on the violations of *Law 15/1999*[261]. In 2004, the *AEPD* defined the IP addresses as "personal data", and therefore, since then, all the data managers in the Internet have to adjourn the information collected in the *Databases Register*, in order to avoid violations, and consequent fines, up to 300,000 euros[262].

Further more, in January 2005, the *AEPD* decided that the information has to be published within one month from its communication to the parties involved, in the interests of transparency, and to promote public awareness

---

[258] Id.
[259] *Real Decreto 994/1999*, de 11 de junio, "por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal".
[260] *Real Decreto 1720/2007*, de 21 de diciembre, "por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal".
[261] "Conozca la Agencia, estructura y funciones", *Agencia Española de Protección de datos* (*www.agpd.es*).
[262] "Carácter de Dato Personal de La Dirección IP" (Informe 327/03), *Agencia Española de Protección de Datos* (*www.agpd.es*).

of its provisions[263]. In the name of public awareness, between 2004 and 2005, the *AEPD* also conducted an active campaign against "spam", imposing fines of up to 30,000 euros for each violation.

Beyond that, in December 2006, the *AEPD* issued a new *Regulation on Video Surveillance*. On the basis of this *Regulation*, in fact, the images obtained from "cameras placed in public places" are considered "personal data", and the data files and images must be therefore protected. Further more, cameras can be used only if other means of surveillance are not readily available, they must be clearly marked, and their records must be destroyed after one month. Private footages, though, are excluded from this *Regulation*[264].

Finally, we must point out that the *Autonomous Communities* of *Madrid*[265], *Catalonia*[266], and of the *Basque Country*[267] have their own *Authorities for Data Protection*, which have to implement also *Ley Organica 15/1999*, though, beyond their autonomous regulations, of course.

32. Digital Privacy in the *EU* and *Directive 2002/58/EC*

As in the *United States*, the digital era had an impact also on the *European Union's privacy* laws, and therefore *Directive 95/46/EC* had to be gradually adjourned and amended. This process started on July 12 2002, with the adoption, by the *European Parliament* and *Council*, of *Directive*

263 "Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre la publicación de sus resoluciones", Agencia Española de Protección de Datos (www.agpd.es).
264 "Guide on Video Surveillance", Agencia Española de Protección de Datos (www.agpd.es).
265 *Agencia de Protección de Datos de la Comunidad de Madrid* (*www.madrid.org*).
266 *Autoritat Catalana de Protecció de Dades* (*www.apd.cat*).
267 *Agencia Vasca de Protección de Datos* (*AVPD, www.avpd.es*).

2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector[268].

This *Directive*, usually, referred to as the "*Directive on privacy and electronic communications*", updated the regulations on personal data processing, and on the protection of *privacy* in several specific sectors of electronic communications. *Directive 2002/58/EC* consisted of a *Preamble* (*Paragraphs 1-49*) and of *21 Articles*.

Further more, *Paragraph 6* of its *Preamble* explained perfectly the necessity of amending the previous legislation: " The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and *privacy*"[269]. For this reason, the *European Legislator* had to adapt *Directive 95/46/EC* "to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and *privacy* for users of publicly available electronic communications services, regardless of the technologies used" (*Preamble, Paragraph 4*)[270].

---

[268] *Directive 2002/58/EC* of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications).
[269] *Preamble, Paragraph 6*, *Directive 2002/58/EC* of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications).
[270] *Preamble, Paragraph 4*, *Directive 2002/58/EC* of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications).

Beyond this, *Directive 2002/58/EC* also expressly required "to repeal" the previous *Directive 97/66/EC*[271] (*Article 19*)[272]. Moreover, the 2002 *Directive* regulated, in a detailed way, the "confidentiality of the communications" (*Article 5*), "traffic data" (*Article 6*), "itemized billing" (*Article 7*), the "presentation and restriction of calling and connected line identification" (*Article 8*), as well as the "location data other than traffic data" (*Article 9*), the characteristics of the "directories of subscribers" (*Article 12*), and also the "unsolicited communications" (*Article 13*)[273].

However, what matters the most for our analysis is the fact that, according to *Article 15*, "*Member States* may adopt legislative measures to restrict the scope of the rights and obligations provided for in *Article 5, Article 6, Article 8(1), (2), (3)* and *(4),* and *Article 9* of this *Directive* when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard *national security (i.e. State security),* defense, *public security,* and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in *Article 13(1)* of *Directive 95/46/EC*"[274].

Therefore, we can notice continuity between *Directive 95/46/EC* and *Directive 2002/58/EC*, especially in balancing *privacy* and *national security*.

---

[271] *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".

[272] *Article 19, Directive 2002/58/EC* of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications).

[273] *Articles 5 - 9, 12, 13, Directive 2002/58/EC* of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications).

[274] *Article 15, Directive 2002/58/EC* of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications).

Though, in order to confirm the trend of keeping *EU* regulations proportionally updated, in regards to the constant technological developments, also the latter *Directive* has been adjourned twice already, by *Directive 2006/24/EC*[275], first, and by *Directive 2009/136/EC*[276], afterwards.

33. Directive 2006/24/EC

Directive 2006/24/EC had the goal of harmonizing the laws of *Member States* "on the retention of telematics' and telephones' traffic data", in order to make them available for the investigation of serious crimes. For this reason, this *Directive* required *Member States* to introduce, for their National providers of electronic communications services, the obligation of retaining their traffic data for a minimum period of six months, up to a maximum of 24 months, for them to be available for the *States*' *National Authorities*, for the prosecution of serious crimes[277].

Moreover, *Directive 2006/24/EC* laid down the rules on: the "obligation to retain data" (*Article 3*), the "access to data" (*Article 4*), the "categories of data to be retained" (*Article 5*), the "periods of retention" (*Article 6*), "data protection and data *security*" (*Article 7*), the "storage requirements for retained data" (*Article 8*), the "*Supervisory Authority*"

---

[275] *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".

[276] *Directive 2009/136/EC* of the European Parliament and of the Council, of 25 November 2009, "amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) no. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws".

[277] *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".

(*Article 9*), the “statistics” (*Article 10*), "future measures" (*Article 12),* and also on the "evaluation" (*Article 14*)[278].

In terms of *privacy* and *security*, therefore, in addition to the measures provided by earlier *Directives 46* and *58*, *Directive 24* stated, in *Article 8*, that the data had to be stored in order to be transmitted without delay to the competent authorities at their request[279]. In order to allow this, *Article 7* established: "Without prejudice to the provisions adopted pursuant to *Directive 95/46/EC* and *Directive 2002/58/EC*, each *Member State* shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data *security* principles with respect to data retained in accordance with this *Directive*: *(a)* the retained data shall be of the same quality and subject to the same *security* and protection as those data on the network; *(b)* the data shall be subject to appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure; *(c)* the data shall be subject to appropriate technical and organizational measures to ensure that they can be accessed by specially authorized personnel only; and *(d)* the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention"[280].

---

[278] *Articles 3 - 10, 12, 14 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".

[279] *Article 8, 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".

[280] *Article 7, 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

However, no matter its correct implementation in individual *Member States*, by the 2009 deadline[281], the *European Court of Justice* recently declared *Directive 2006/24/EC* invalid, specifically on April 8 2014[282]. In fact, the *Court* believes that this *Directive* had a significant effect on the fundamental rights laid down in the *European Charter*, as the respect for private life and the protection of personal data, exceeding the limits imposed by the proportionality principle: "If a limitation of fundamental rights can be justified by the pursuit of common interests, such as fighting and combating terrorism and other serious crimes, this must be done by limiting the intervention to what is strictly necessary to achieve those objectives"[283].

In addition, according to the *Court*, the *Union Legislator* did not take into account this principle, while regulating the obligation to retain traffic data. In particular, the *Directive* extended the obligation to retain indiscriminately all the traffic data, without making any distinction in the categories of data stored and/or of the persons concerned, in regards to the objective pursued. Further more, the *Directive* did not indicate the criteria

---

available electronic communications services or of public communications networks and amending Directive 2002/58/EC".

[281] The implementation deadline was March 15 2009; *Italy*, for example, implemented *Directive 2006/24/EC* through its "Decreto Legislativo 30 maggio 2008, n. 109 - Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE"; this Legislative decree can be read at *www.governo.it*.

[282] *Joined Cases C-293/12 and C-594/12* - Judgment of The Court (Grand Chamber), 8 April 2014 - "(Electronic communications; Directive 2006/24/EC; Publicly available electronic communications services or public communications networks services; Retention of data generated or processed in connection with the provision of such services; Validity; Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union), Requests for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, received at the Court on 11 June and 19 December 2012, in the proceedings Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others".

[283] Id.

according to which *Member States* should have regulated the duration of the retention period, between a minimum of 6 months to a maximum of 24 months, in order to ensure that such term would not go beyond what was "strictly necessary".

More profiles of illegality have been found in the fact that the *Directive* lacked of specific predictions, such as measures to be taken, in order to avoid the risk of "unauthorized access" or "unlawful use of the stored traffic data", and "the obligation to retain data inside the *EU*".

Finally, in declaring invalid *Directive 2006/24/EC*, the *Court* did not limit the temporal effects of its decision, as the *Advocate General* had requested [284]. The impact of this decision on the individual *National Legislation*, which implemented *Directive 2006/24/EC*, therefore, is still uncertain. As already mentioned, though, there have been further amendments in the *European* legislation, specifically through the latest *Directive 2009/136/EC*[285].

34. Directive 2009/136/EC

Directive 2009/136/EC, designed to meet the needs of digital technologies, amended the previous *European Directives on Data Protection*, in regards to all the electronic communications issues, affecting the private sphere. Its purpose is to improve transparency and *security* for users.

---

[284] Id.

[285] *Directive 2009/136/EC*, of November 25 2009, "amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws".

Among the changes, the main ones concerned the use of "cookies", which allow us to store logins, passwords and bookmarks[286]. This feature is very convenient for users, but it can also be used to follow the surfing behavior of a person in the network, thus allowing online advertisers to set up user profiles, and to personalize advertising for each user/consumer, through cookies distributed over several sites. This procedure is called "Online Behavioral Advertising" (OBA).

However, *Directive 2009/136/EC* replaced the prior "Opt-out" system with a so-called "Informed-Consent" solution, i.e. an "Opt-in" (optional inclusion) system, which provides the user with detailed information about the type and purpose of his data processing[287]. Further more, *Directive 2009/136/EC* excluded those procedures, whose only purpose is to carry out the transmission of a communication over an electronic communications network, in order to provide a specifically requested service (so-called "Session-Cookies").

The ways to ask the user's consent, for the setting of cookies, are set out in the *Preamble* of the *Directive*, according to which, the "provision of information" and the "offer of the right to refuse" "should be clear and understandable". If technically feasible and effective, the consent of the user "can be expressed by using the appropriate settings of a browser or of other applications"[288].

---

[286] Id.

[287] Id.

[288] *Preamble, Directive 2009/136/EC*, of November 25 2009, "amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws".

The consequences and significance of these provisions, though, are quite controversial. In fact, many *National Authorities* for the supervision of *privacy*, including the *Italian "Garante"*, have heavily criticized this "opt in" system for the cookies, because they consider it inconsistent with the dynamics of the Internet and detrimental the *European* companies, which operate online, compared to their overseas competitors, which are not subjected to these limitations[289].

Further more, while some *EU Member States* have implemented the *Directive* into *National Law*[290], other *Countries* have not been able to do so. In fact, it is not easy to find a way of enabling them to comply with the legal provisions of the "Informed Consent" rule, without unduly limiting the ease of navigation.

35. Proposed Changes to *EU*'s *Privacy*

No matter the late implementation by many *Member States*, and the non-implementation of many others, also *Directive 2009/136/EC* should not complete the *EU* policy on *privacy* and *National security*. In fact, on January 25 2012, the *European Commission* proposed both a new *Directive* and a new *Regulation*, in order to amend, once and for all, Data Protection regulations in the *EU*[291].

---

[289] "Faq in materia di cookie", *Garante per la protezione dei dati personali* (*www.garanteprivacy.it*).
[290] *Italy*, for example, has implemented *Directive 2009/136/EC*, through its "Decreto legislativo 28 maggio 2012, n. 69, Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori. (12G0090)", only in 2012. This Italian Legislative decree is available at *www.garanteprivacy.it*.
[291] "Commission proposes a comprehensive reform of the data protection rules", 25/01/2012, Data Protection - Newsroom, *European Commission* (*www.ec.europa.eu*).

Beyond the already mentioned technological developments, the *28 EU Member States* have implemented the previous rules differently, which, therefore, resulted also in enforcement divergences. For these reasons, the *Commission* proposed one single law, which "will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in *Europe*"[292].

The proposed *Regulation* will replace *Directive 95/46/EC*[293], and the proposed *Directive* will regulate data treatments for Justice and Police purposes (currently excluded from the scope of *Directive 95/46/EC*)[294]. We have to keep in mind that *EU Regulations* are immediately enforceable; they do not need to be implemented by the *Member States*, differently from the *Directives*. For this reason, they may ensure a better harmonized *EU*-wide law.

Some of the major innovations of the proposed *Regulation*, compared to *Directive 95/46/EC*, are significant additions to the fundamental definitions ("genetic data", "biometric data"), and the introduction of the principle by which *EU* law applies also to personal data processing, carried

[292] Id.
[293] "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels, 25.1.2012 com (2012) 11 final 2012/0011 (cod), *European Commission*.
[294] "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data", com/2012/010 final - 2012/0010 (cod), *European Commission*.

out of the *EU*, whether related to the supply of goods or services to *EU* citizens, or such as to enable the monitoring of the *EU* citizens' behavior[295].

Further more, the new *Regulation* should establish the right of "data portability" for interested parties (for example, in case someone intends to transfer his data from one social network to another), but also the "right to be forgotten", i.e. to decide what information can continue to circulate (in particular in the online world), after a certain period of time, except for some cases (for example, when complying with legal requirements, ensuring the exercise of freedom of expression, or allowing a historical research).

Another novelty of the proposed *Regulation* is the abolishment of the obligation to notify the owners of databases on personal data, by replacing it with the appointment of a "data protection officer" (in charge of data protection, according to the terminology of *Directive 95/46*), for all the public and the private entities, with a certain number of employees.

Moreover, also the concept of "*privacy* impact assessment" will be introduced, beyond the general "*privacy* by design" principle (i.e. the provision of measures to protect data, during the design stage of a product or software). The new *Regulation* shall also establish the obligation, for all the data holders, to notify the competent *Authority* of the “personal data breaches". In fact, the *Regulation* proposal redefines the powers and the independence requirements of the National *Supervisory Authorities*. The opinion of these *Authorities* will be essential, in order to adopt other

[295] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels, 25.1.2012 com (2012) 11 final 2012/0011 (cod), *European Commission*.

regulatory instruments, or any law that has an impact on the protection of personal data[296].

Regarding the proposed *Directive*, instead, it should replace the *Framework Decision (2008/977/JHA)*, currently in force, and which governs data processing by the Police and the Judicial Authorities. We should emphasize that the provisions of this *Directive* shall apply, in general, to all personal data processing, carried out in a *Member State* for such "institutional" purposes, while the *Framework Decision* only covers the exchange of information between the competent *Authorities* of the *Member States*, and the subsequent data treatment, exchanged in that context[297].

This eventual *Directive* will also incorporate many of the proposed *Regulation*'s contents, including the definitions of "personal information", "treatment", and so on. It will, however, contain specific provisions on the holders' liability and on the obligations imposed on them, regarding transparency and access. Further more, it will establish the criteria of legitimacy for data treatments, and the mechanisms for mutual cooperation between the *National Supervisory Authorities*. As already mentioned, its provisions must be implemented through appropriate *National* laws[298].

Finally, the process for the approval of the two proposed regulatory instruments should consist in a joint intervention of the *European Parliament* and the *EU Council*, in accordance to the so called "co-decision

---

[296] Id.
[297] "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data", com/2012/010 final - 2012/0010 (cod), *European Commission*.
[298] Id.

procedure" (now defined by the *Treaty of Lisbon* "legislative procedure")[299]. Therefore, let us review the most important stages of this process, up to date.

First of all, in July 2013, during the *JHA Council*, in *Vilnius*, the *French* and *German Ministers of Justice* have issued a joint statement urging the *EU* to undertake a rapid and ambitious action for the legislative package on the protection of personal data. *Spain,* the *Netherlands, Austria, Italy* and *Poland* have expressed their support for the Franco-German proposal[300].

Further more, on December 6 2013, the *Council of Justice and Home Affairs* met to discuss the "one-stop-shop" mechanism. Many *Member States*, including *Italy*, have expressed some concerns about it[301].

Regarding the 2014 developments, instead, on March 4 the *JHA Council* met to discuss "territorial scope", "international data transfers", "data aliases", "data portability", and the "data processing and profiling obligations"[302]. On March 12, then, the *European Parliament*, meeting in its plenary session in *Strasbourg*, approved, on first reading, the proposed *Regulation,* with 621 votes to 10 and 22 abstentions, and the *Directive,* with 371 votes to 276 and 30 abstentions[303]. On June 6, however, there has been another *JHA Council* meeting, in *Luxembourg*, during which the *Ministers* have reached a partial agreement on the *Fifth Chapter* of the proposed *Regulation*.

---

[299] "Article 289 of the Treaty on the Functioning of the EU now only refers to two types of legislative procedure: ordinary legislative procedure; special legislative procedures. In addition, the Treaty of Lisbon introduces 'passerelle clauses'. These clauses enable the ordinary legislative procedure to be generalized, under certain conditions, to areas that were initially outside its scope", *Legislative procedures* (*www.europa.eu*).

[300] "Informal Justice Council in Vilnius", *European Commission* - MEMO/13/710, 19/07/2013, (*www.europa.eu*).

[301] "Press Release, 3279th Council Meeting, Justice and Home Affairs", Brussels, 5 and 6 December 2013, 17342/13 (OR. en), Presse 534 PR CO 64, *Council of the European Union* (*www.consilium.europa.eu*).

[302] "Press Release, 3298th Council Meeting, Justice and Home Affairs", Brussels, 3 and 4 March 2014, 7095/14 (OR. en) Presse 106 PR CO 11, *Council of the European Union (www.consilium.europa.eu).*

[303] "Texts adopted, Wednesday March 12, 2014" - Strasbourg, *European Parliament* (*www.europarl.europa.eu*).

In addition, there was also another debate on the "one-stop-shop" mechanism[304].

Finally, on July 10, an informal *Council of the EU Ministers of Justice* was held in *Milan*. In order to overcome a block in the *Council*'s work, it seems that the *Italian Presidency of the EU* (formally commenced on July 1 2014) has proposed to provide *Germany*, a key player in the negotiations, certain guarantees on the treatment of public enterprises in the future legislation.

Since the beginning of the debate, in fact, *Germany* has always raised the issue of equal treatment between the private and the public sectors, with the aim of protecting the *German National* legislation, on the protection of citizens' data, among the most strict in *Europe*, as already mentioned. Therefore, the *Council* should, hopefully, reach an overall agreement by the end of the *Italian Presidency of the EU* (December 2014)[305].

36. Boundaries between *Privacy* and *Security* in the *EU*

Up to date, no matter the imminent adoption and implementation of the proposed *Regulation* and *Directive*, discussed so far, and the other *Directives* adopted, the relationship between *individual privacy* and *national security* in *Europe* is still profoundly anchored to the limits of *Article 13* of *Directive 95/46/EC*[306], also recalled by *Article 15* of *Directive 2002/58/EC*[307].

---

[304] "Press Release, 3319th Council Meeting, Justice and Home Affairs", Brussels, 5 and 6 June 2014, 10578/14 (OR. en) Presse 328 PR CO 31, *Council of the European Union* (*www.consilium.europa.eu*).
[305] "Riforma della normativa europea sulla protezione dei dati personali", Aggiornamento iter legislativo, *Delegazione di Confindustria presso l'Unione europea* (*www.confindustria.eu*).
[306] *Article 13, Directive 95/46/EC* - "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", of the *European Parliament* and of the *Council*, of 24 October 1995. See *Paragraph 16.*
[307] *Article 15, Directive 2002/58/EC* of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications). See *Paragraph 23.*

In fact, these *Articles* do not make it easy to distinguish, in practice, whether the transfer of *European* citizens' data to other *Countries*, for example, involves their personal relationships and the proper functioning of the *European* internal market, or whether that transfer is due to the protection of individuals' fundamental rights and freedoms, in regards to the needs of *National security*, national defense or public order.

However, it is important to keep in mind, that, differently from the *U.S. Federation*, it will always be hard for a *Union* regrouping *28 Member States* (and their autonomous legal traditions) to forecast all the possible "*privacy* breaches", by regulating them *ex* ante. Though, the common legal traditions of the *Member States*, and the historical background of the *European Continent*, have fortunately been forcing the *EU Commission, Parliament* and *Council* to reduce considerably the cases where *national security* can limit *individual privacy*.

Further more, the case of *Germany*'s resistance to the implementation of the proposed *Regulation* and *Directive*, unless they protect the private and the public enterprises equally[308], is a perfect example of the balance that has to constantly be reached, in a context with so many *State-Actors*. Provided this, we shall analyze the recent "*Datagate*" scandal, and the different reactions of the *U.S.* and the *EU*, in the next *Chapter*. This will allow us to fully confront their *privacy-security* policies, afterwards.

[308] See *Paragraph 20*.

Chapter III

The *Datagate Scandal*:

Individual Privacy vs. *National Security*

37. The *Scandal*

It was June 6 2013 when *The Guardian* newspaper published the scoop on the *NSA*, the *National Security Agency* of the *United States*. The *NSA* had forced the phone operator *Verizon* to provide it with the telephone data of its subscribers. It was "metadata", not the content of the conversations, therefore, but data regarding who calls whom, from where, and for how long[309].

The next day, *The Washington Post* and *The Guardian* revealed also that the *NSA* and the *FBI* had requested *Microsoft*, *Google*, *Yahoo*, and *Facebook* to access files, photos, videos, emails, and conversations, traded on their platforms, for the top-secret "*PRISM*" *Program*, launched under the *George W. Bush* presidency, and renewed in 2012. These giant web companies initially denied having authorized access[310], though, on June 15 2013, *Facebook*, *Microsoft*, *Apple* and *Yahoo*[311] confirmed they had received information requests about their users from *U.S.* Agencies[312].

---

[309] Greenwald G. - "NSA collecting phone records of millions of Verizon customers daily, Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama", *The Guardian*, June 6, 2013.

[310] Greenwald G. and MacAskill E. - "NSA Prism program taps in to user data of Apple, Google and others, Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook, Companies deny any knowledge of program in operation since 2007", *The Guardian*, June 7, 2013.

[311] Only on September 11, 2014 the *Washington Post* has revealed that: "The U.S. government threatened to fine Yahoo $250,000 a day in 2008 if it failed to comply with a broad demand to hand over user communications — a request the company believed was unconstitutional — according to court documents unsealed…that illuminate how federal officials forced American tech companies to

Further more, on June 21, *The Guardian* launched another bombshell, this time involving the *United Kingdom*. In fact, it revealed the existence of "*Tempora*", a *British Surveillance Program*, which intercepted worldwide communications, over fiber optic cables. The content of these interceptions was stored for 3 days, but their metadata was stored up to 30 days[313]. Beyond this, other documents, uncovered by the *NSA* whistleblower, *Edward Snowden*, revealed the *GCHQ*'s (*British NSA* equivalent) surveillance of *G20* Delegates' emails and phones, at two *G20 London Summits*, in 2009. Apparently, at the time, phones were monitored and fake Internet cafes were set up, in order to gather information from allies[314].

The news that the communications of millions of *American* and *European* citizens was under the *U.S.* and *UK Governments*' control, therefore, appeared on the first pages of all the newspapers, and has toured the World, giving rise to what journalists have called "the *Datagate* scandal".

38. The *Whistleblower*

Initially, the source of *The Guardian* was anonymous. However, a few days after the *Scandal*, precisely on June 10, *Edward Snowden* revealed he was the informer. The 29 years old, former employee of the *NSA*, confessed: "I am the *Whistleblower* who told the matter (...) I do not want to live in a

---

participate in the National Security Agency's controversial PRISM program" (Timberg C. - "U.S. threatened massive fine to force Yahoo to release data", *The Washington Post*, September 11, 2014).

[312] Barberis E. - "Il caso Datagate", *La Stampa,* 2013.

[313] MacAskill E., Borger J., Hopkins N., Davies N. and Ball J. - "GCHQ taps fibre-optic cables for secret access to world's communications, Exclusive: British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls, and shares them with NSA, latest documents from Edward Snowden reveal", *The Guardian*, June 21, 2013.

[314] MacAskill E., Davies N., Hopkins N., Borger J. and Ball J. - "GCHQ intercepted foreign politicians' communications at G20 summits", *The Guardian*, June 17, 2013.

World where everything you do and say is recorded. I decided to reveal everything without hiding behind anonymity because I hate the secret"[315].

The *United States Government*, therefore, asked for his extradition, and *Snowden* was forced to leave *Hong Kong*, where he had been since May 2013[316]. In fact, he was officially accused of espionage, theft and illegal use of *Government* property. After leaving *Hong Kong* "legally", in the direction of *Moscow*, *Snowden* asked *Cuba*, *Ecuador* and almost 20 other *Countries* to grant him asylum. Though, he had to stay in the transit area of *Moscow*'s airport, since *Washington's Authorities* withdrew his passport. In those days, in fact, *Russian* President *Putin* confirmed the presence of *Snowden* in *Moscow*'s airport, but denied the *U.S.* his extradition: "He is a free man", stated *Putin*[317].

On July 3 2013, there was a so-called "diplomatic incident". Some *Countries* (including *Italy*, *France*, *Spain* and *Portugal*), believing that *Snowden* was leaving *Russia*, on board of *Bolivian* President *Morales*' jet, prohibited it to fly over their territories. For this reason, *Morales* remained stuck in *Vienna* for 14 hours, but the *Whistleblower* was not on the plane.

Further more, in response to the *Snowden*'s several asylum requests, *Italian* Foreign Minister *Emma Bonino* announced: "there are no conditions to grant *Snowden* asylum"[318]. *Venezuela* and *Nicaragua*, instead, declared that they were available to grant it. However, as already mentioned, *Snowden*

---

[315] Greenwald G., MacAskill E. and Poitras L. - "Edward Snowden: the whistleblower behind the NSA surveillance revelations, The 29-year-old source behind the biggest intelligence leak in the NSA's history explains his motives, his uncertain future and why he never intended on hiding in the shadows", *The Guardian*, June 10, 2013.
[316] Branigan T. and Elder M. - "Edward Snowden leaves Hong Kong for Moscow, NSA whistleblower left on Aeroflot flight to Moscow, Hong Kong government confirms, two days after US charged him with espionage", *The Guardian*, June 23, 2013.
[317] Lally K. and Englund W. - "Putin: No grounds to extradite Snowden", *The Washington Post*, June 25, 2013.
[318] Maurizi S. - "Datagate. Bonino, perché non risponde?", *Espresso*, July 9, 2013.

had no passport, and, therefore, could not leave *Russia*, or even book a flight. On August 1 2013, though, *Russia* granted *Snowden* a one-year visa. He could finally leave *Moscow's Sheremetyevo* airport, where he had been blocked from June 23, and officially enter *Russia*[319].

Meanwhile, *Glenn Greenwald*, *The Guardian* journalist who made the scoop, guaranteed that thousands of documents from the *NSA* were in the hands of certain trustees: "if anything happens to *Snowden*", he said, just as what *Julian Assange* had done during the *WikiLeaks* scandal[320]. Since then, however, nothing has threatened *Snowden* in *Russia*. On the contrary, he was awarded the *Integrity Award* from the *Sam Adams Associates*, for "Integrity in Intelligence", at the end of last year[321].

No matter the "right to the freedom of press", mentioned in *Chapter I*, though, not all of the journalists have been praising *Edward Snowden*. In fact, in the *UK*, for example, the *Daily Mail* launched a press campaign against the publication of his revelations by *The Guardian*. It accused the *Whistleblower* and the *Publishing Newspaper* of "destabilizing *National security*" and of "promoting terrorism"[322]. However, *The Guardian* reacted strongly in their defense, by publishing the opinion of thirty newspapers' Directors from all over the World, on the "right of readers to be informed".

Snowden, on his behalf, launched a *security* alert and insisted, in a series of short videos published on the *WikiLeaks* website: "The *Monitoring*

---

[319] Fantz A., Black P. and Martinez M. - "Snowden out of airport, still in Moscow", *CNN*, August 2 2013.
[320] Lake E. - "Greenwald: Snowden's Files Are Out There if 'Anything Happens' to Him", Politics, *The Daily Beast*, June 25, 2013.
[321] Lavender P. - "Edward Snowden Receives Sam Adams Award", *Huffington Post*, December 10, 2013.
[322] Doyle J. and Greenwood C. - "Guardian may face terror charges over stolen secrets: Met Deputy Commissioner confirms she is investigating whether newspaper broke the law", *Daily Mail*, December 3, 2013.

Program, used by the *United States* to control the phone and Internet connections in the *World*, makes people less safe". Finally, after considering his mission "accomplished"[323], *Edward Snowden* was recently granted by the *Russian Government* a three-year residency permit, in August 2014[324]. But let us now specifically analyze the *PRISM* and *Tempora Programs,* first, and the *U.S.'* and *EU's* reactions to the *Scandal*, afterwards.

39. PRISM

PRISM is a mass electronic surveillance data mining *Program*, designed by the *U.S. National Security Agency (NSA)*, in order to combat terrorism[325]. Despite the news has spread only in June 2013, the *PRISM Program* was launched in 2007, already[326]. Basically, this *Program* extended the surveillance of "potential terrorists" to millions of *American* citizens, by monitoring communications within the *United States*, or between the *United States* and foreign *Countries*[327].

In fact, the *PRISM Program* registered Internet communications, under *Section 702* of the *FISA Amendments Act* of 2008, which allowed the *NSA* to request Internet companies, such as *Google Inc.*[328], to turn over any data,

---

[323] Gellman B. - "Edward Snowden, after months of NSA revelations, says his mission's accomplished", *The Washington Post*, December 23, 2013.
[324] Luhn A. and Tran M. - "Edward Snowden given permission to stay in Russia for three more years", *The Guardian*, August 7, 2014.
[325] Gellman B. and Poitras L. - "US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program", *The Washington Post*, June 6, 2013.
[326] Chappell B. - "NSA Reportedly Mines Servers of US Internet Firms for Data". *The Two-Way (blog of NPR)*, June 6, 2013.
[327] Whittaker Z. - "PRISM: Here's How the NSA Wiretapped the Internet", *ZDNet*, June 8, 2013.
[328] Greenwald G. and MacAskill E. - "NSA Prism program taps in to user data of Apple, Google and others, Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook, Companies deny any knowledge of program in operation since 2007", *The Guardian*, June 7, 2013.

matching the court-approved search terms[329]. The *NSA*, therefore, could target the encrypted communications, when they traveled across the Internet backbone, in order to analyze stored data, that telecommunication filtering systems had discarded earlier, and also in order to handle data more easily[330].

The "convenience" of the *PRISM Program*, however, consisted in being able to intercept the communications between users and servers that were located in different *Countries*. From this point of view, it has been very strategic, since most of the *World*'s communications, between users in different *Countries*, go through the *United States* or anyway through a *United States ISP*[331], allowing *PRISM* to store even more data. Therefore, almost all the communications could potentially be intercepted, unless strong encryption systems (such as *PGP*[332], *Tor*[333] and similar means) are used[334].

Further more, the *PRISM Program* was also accused of carrying out cyber attacks on private networks, and to install *Trojans*[335] on targeted

---

[329] Gellman B. and Soltani A. - "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". *The Washington Post*, October 30, 2013.

[330] Valentiono-Devries J. and Gorman S. - "What You Need to Know on New Details of NSA Spying", *The Wall Street Journal*, August 20, 2013.

[331] "An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned". ("Internet service provider", *Wikipedia*).

[332] "Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications". ("Pretty Good Privacy", *Wikipedia*).

[333] "Tor (previously an acronym for The Onion Router) is free software for enabling online anonymity and resisting censorship. It is designed to make it possible for users to surf the Internet anonymously, so their activities and location cannot be discovered by government agencies, corporations, or anyone else". ("Tor (anonymity network)", *Wikipedia*).

[334] Gorman S. and Valentiono-Devries J. - "New Details Show Broader NSA Surveillance Reach - Programs Cover 75% of Nation's Traffic, Can Snare Emails", *The Wall Street Journal*, August 20, 2013.

[335] "A Trojan horse, or Trojan, in computing is a generally non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the

computers, in order to gain control of certain users' data[336]. Finally, the *PRISM Program* had a strict connection with *Tempora*, its *British* equivalent[337].

40. Tempora

As already mentioned, the *Tempora Program* is a *Surveillance Program* of the *UK Government Communications Headquarters*, or simply *GCHQ*, the spy *Agency* dedicated to intelligence and information gathering. It is, therefore, the *British* equivalent to the *NSA*, basically[338]. For this reason, when *Snowden* was interviewed by *The Guardian*, he spoke of the "indiscriminate wider surveillance program in the history of mankind". "It's not just a problem of the *United States*. *Britain* has a very important role in this struggle", he added. ''They (the *British*) are worse than the *Americans*", the *Whistleblower* concluded[339].

In fact, the ambition of the global espionage carried out by the *United Kingdom* is testified from the names chosen for the *GCHQ*'s *Tempora* documents, revealed by *Snowden*, respectively called "Mastering the Internet" and "Global Telecoms Exploitation". Apparently, the *GCHQ* was able to store any kind of data: phone calls, *Facebook* posts, e-mails, and any Internet-based activity.

---

nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Anatolia, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers". ("Trojan horse (computing)", *Wikipedia*).

[336] Braun S., Flaherty A., Gillum J. and Apuzzo M. - "Secret to PRISM Program: Even Bigger Data Seizures", *Associated Press*, June 15, 2013.

[337] Staff - "Datagate, Gb spia tutto il mondo sui cavi di fibra ottica e collabora con Nsa", Blitz Quotidiano, June 21, 2013.

[338] Shubber K. - "A simple guide to GCHQ's internet surveillance programme Tempora", Politics, *Wired UK*, June 24, 2013.

[339] Staff - "Datagate, Gb spia tutto il mondo sui cavi di fibra ottica e collabora con Nsa", Blitz Quotidiano, June 21, 2013.

Further more, the *British* newspaper revealed that, in cooperation with the *United States Authorities*, a total of 850 thousand *NSA* employees and private contractors have had access to the *GCHQ*'s database. The documents also revealed that, only in 2012, the *GCHQ* was able to handle 600 million "telephone events" per day, and was linked to more than 200 fiber optic cables, with the ability to process data simultaneously from at least 46 of those cables[340]. In theory, this gave *GCHQ* access to a flow of 21.6 petabytes in a day, equivalent to 192 times the *British Library*'s entire book collection"[341]. Beyond the obvious International criticism, however*, Edward Snowden's* revelations on the two *Programs* lead to *National* inquiries, of course.

41. Reactions in the *U.S.*

The first statement of *Obama* in regards to the *Datagate* scandal, issued on June 7 2013, stressed the legality of the *Program* for the information collection by the *Intelligence Agenci*es, defining it "not secret, but reserved", and anyways authorized by *Congress*. The *American President* also said that the information was safe from external intrusions, and that he was convinced the *Surveillance Program* would help prevent terrorist attacks, having to find a "balance between *privacy* and *security*". Finally, *Obama* reiterated that the *PRISM Program* was "under close supervision of *Congress*", and, referring to *Snowden*, on the run, he added: "We'll get him"[342].

At the same time, though, the *U.S. Congress* called on the *Government* to give explanations on the *PRISM Program*. Most of the *Congressmen*, in fact,

---

[340] Id.
[341] Bump P. - "The UK Tempora Program Captures Vast Amounts of Data — and Shares with NSA", *The Wire*, June 21, 2013.
[342] Staff - "Obama defends Internet surveillance programs - video", *Reuters*, Saturday 8 June 2013.

both Democrats and Republicans, claimed that they had never heard of the *Program*, "a system that amounted to spying on *Americans*", until *Snowden*'s revelations[343].

For this reason, the *Director* of the *NSA*, General *Keith Alexander*, defended himself, by saying that the *Department of Justice* and the *Congress* were in control of the project[344]. "It is much more important for this *Country* that we defend this *Nation* and take the beatings, than it is to give up a *Program* that would result in this *Nation* being attacked," General *Alexander* added, referring to criticism of his *Agency*, during the *Congress* hearing[345]. Beyond this, the *NSA* submitted to the *Committee on Intelligence* of the *American Congress* 50 cases, in which the *Program* revealed by *Snowden* had contributed to the "understanding and in many cases to disrupt" terrorist plots, in the *U.S.* and in 20 other *Countries*.

Further more, several other *U.S. Public Authorities* have defended the *NSA PRISM Program*. For example, Republican Congressman *Peter King*, in a *NBC* interview, stated: "I think the *President* (*Obama*) should stop asking for forgiveness, and stop being defensive. We have no *Intelligence Programs* for fun. We use them to gather valuable information, that help not only us, but also the *Europeans*"[346]. In the *CNN Program* "State of the Union", then, *Mike Rogers*, *Chairman of the Intelligence Committee of the House of Representatives*, moved in the same direction, by commenting: "the *Safety*

---

[343] Roberts D., Ackerman S. and Travis A. - "NSA surveillance: anger mounts in Congress at 'spying on Americans'", *The Guardian*, June 12, 2013.
[344] Bacchiddu P. - "Datagate, tutte le tappe dello scandalo, Le rivelazioni di Edward Snowden al Guardian, la difesa della Casa Bianca, le risposte carenti della Nsa, le reazioni degli alleati, la fuga in Russia del whistleblower. Nella nostra timeline tutte le tappe principali della vicenda", Timeline, *Espresso,* 2013.
[345] Zakaria T. and Charles D. - "NSA chief defends agency amid U.S. spy rift with Europe", *Reuters*, October 29, 2013.
[346] Miranda R. - "Datagate, la furbetta strategia dell'Europa", *Formiche*, October 29, 2013.

Programs of the *United States* are a good thing, because they protect our *security* and that of our *European Allies*"[347].

However, the majority of the *American* citizens and of their *Representatives* was upset by the contents of *Edward Snowden*'s revelations. For example, *Dianne Feinstein*, *Chairman of the U.S. Senate Intelligence Committee*, said she was "totally against" monitoring the communications of the *U.S.*-Allied Leaders, of which she found out through the *Datagate Scandal*. Further more, she stated: "it is clear that some surveillance activities have been conducted for over a decade, and the *Senate Intelligence Committee* has not been informed in a satisfactory manner"[348]. Finally, she assured that the *NSA* would completely revise its data collection methods[349].

Beyond her, one of the most active protesters in the battle against the *NSA's Surveillance Program* was definitely Senator *Ron Wyden*. In fact, in June 2012 (one year prior to the *Scandal*), the Democratic *Senator* had already asked the *NSA* an estimate of the number of *Americans* being spied on, during the previous year. His request was rejected by the *Agency*, because it would have been "an invasion of *privacy*", to reveal who had been spied upon[350]. In March 2013, *Wyden* had then asked *James Clapper*, the *Director* of the *NSA*, if the *Agency* was gathering data on millions of *Americans*. *Clapper* had replied "No, sir, not wittingly"[351]. Therefore, after 4 years, during which the *Senator* had been trying to make the legal interpretation of the *Foreign Intelligence*

---

[347] Id.
[348] Staff - "Datagate, 'Sbaglio spiare i leader'", *TGCOM24*, October 28, 2013.
[349] Miranda R. - "Datagate, la furbetta strategia dell'Europa", *Formiche*, October 29, 2013.
[350] Puliafito A. - "Datagate: il Washington Post e il New York Times contro Obama", *Polis Blog*, August 10, 2013.
[351] Macaskill E., Dance G., Cage F. and Chen G. - "NSA Files: Decoded, What the revelations mean for you.", *The Guardian*, November 1, 2013.

Surveillance Court on *Section 215* of the *Patriot Act* public, the documents revealing it, were finally published, thanks to *Edward Snowden*[352].

42. ACLU vs. *NSA*

It was the *American Civil Liberties Union*, "the guardian of the *Nation*'s liberty"[353], however, to proceed against the *NSA*, in the name of the *Americans' privacy*. In fact, on June 11 2013, a few days after the *Scandal*, it filed a lawsuit challenging the constitutionality of the *National Security Agency*'s mass collection of *Americans*' phone records, together with the *NYCLU*[354]. Further more, both *Unions* were current or recent *Verizon* business customers, which, as we mentioned earlier, had been forced to give the *NSA* access to their phone records[355].

The *ACLU* has been trying to demonstrate that "the *NSA*'s aggregation of metadata constitutes an invasion of *privacy* and an unreasonable search and is, therefore, unconstitutional under the *Fourth Amendment*". Beyond this, the *Union* has also been evidencing that "the call-tracking program also violates the *First Amendment*, because it vacuums up sensitive information about associational and expressive activity"[356].

However, the lawsuit brought to the *New York's District Court* by the *American Civil Liberties Union*, soon after the *Scandal*'s eruption, took a turn in favor of the *NSA*, in December 2013. In fact, Judge *Pauley*, referring to the

---

[352] Puliafito A. - "Datagate: il Washington Post e il New York Times contro Obama", *Polis Blog*, August 10, 2013.
[353] Staff - "About the ACLU", *American Civil Liberties Union Website*.
[354] Staff - "ACLU v. Clapper – Challenge to NSA Mass Call-Tracking Program", *American Civil Liberties Union Website*.
[355] Greenwald G. - "NSA collecting phone records of millions of Verizon customers daily, Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama", *The Guardian*, June 6, 2013.
[356] Staff - "ACLU v. Clapper – Challenge to NSA Mass Call-Tracking Program", *American Civil Liberties Union Website*.

privacy protections enshrined in the *Fourth Amendment* of the *U.S. Constitution*, stated that it needed to be balanced with the *Government*'s need to prevent terrorist attacks. "The right to be free from searches is fundamental but not absolute", he said. "Whether the *Fourth Amendment* protects bulk telephony metadata is ultimately a question of reasonableness"[357].

Beyond this, the *New York Judge* argued that "*al-Qaida*'s bold jujitsu strategy, to combine a seventh century ideology with the twenty-first century technology", obliged the *U.S. Government Intelligence Agencies* to "push the *boundaries of privacy*". "As the *September 11 Attacks* demonstrate, the cost of missing such a threat can be horrific", he wrote in the ruling. "Technology allowed *al-Qaida* to operate decentralized and plot international terrorist attacks remotely. The bulk telephony metadata collection *Program* (*PRISM*) represents the *Government*'s counter-punch: connecting fragmented and fleeting communications to re-construct and eliminate *al-Qaida*'s terror network", District Judge *Pauley* then added[358].

Further more, he explained: "The *ACLU* argues that the category at issue (all telephony metadata) is too broad and contains too much irrelevant information. That argument has no traction here. Because without all the data points, the *Government* cannot be certain it is connecting the pertinent ones". "There is no way for the *Government* to know which particle of telephony metadata will lead to useful counterterrorism information ... Armed with all the metadata, *NSA* can draw connections it might otherwise never be able to find. The collection is broad, but the scope of

---

[357] Roberts D. - "NSA mass collection of phone data is legal, federal judge rules", *The Guardian*, December 27, 2013.
[358] Id.

counterterrorism investigations is unprecedented", the *District Judge* concluded[359].

However, the *ACLU Deputy Legal Director*, *Jameel Jaffer*, stated they would appeal this decision: "We are extremely disappointed with this decision, which misinterprets the relevant *Statutes*, understates the *privacy* implications of the *Government*'s surveillance and misapplies a narrow and outdated precedent to read away core constitutional protections"[360]. "As another *Federal Judge* and the *President*'s own review group concluded last week, the *National Security Agency*'s bulk collection of telephony data constitutes a serious invasion of *Americans' privacy*. We intend to appeal and look forward to making our case in the second circuit", *Jaffer* added.[361]

Finally, Judge *Pauley* precised that his ruling did not mean it was right to continue with the *Program*, which he acknowledged was a "blunt tool", that "imperils the civil liberties of every citizen", if unchecked. "While robust discussions are under way across the *Nation*, in *Congress*, and at the *White House*, the question for this *Court* is whether the *Government*'s bulk telephony metadata *Program* is lawful. The *Court* finds it is", he wrote. "But the question of whether that *Program* should be conducted is for the other two coordinate branches of *Government* to decide", concluded *Pauley*[362].

In light of this and other essential rulings, *American* politicians, judges and other citizens may continue their daily dispute on whether the *PRISM Program* has violated or not the *U.S. Constitution*, and, in general, their *Individual privacy*. However, even among those who believe the *American Intelligence* has effectively breached *privacy* rules, many still argue that it

[359] Id.
[360] Id.
[361] Id.
[362] Id.

was “necessary”, since it helped preventing terrorist attacks, and, therefore, safeguarding *National security*.

43. Reactions in *Europe*

On the other side of the *Atlantic Ocean*, the *EU Member States*’ reactions to the *Datagate* scandal were diverse, but definitely “rougher”, to say the least. This was due in particular to the continuously shocking news. Beyond *The Guardian*’s revelations, in fact, also the *German* newspaper *Der Spiegel* and the *French* newspaper *Le Monde* “added fuel to the fire”.

On one hand, *Der Spiegel* revealed that, in addition to *Germany* and *France*, also *Italy* was among the intercepted *European Countries*, by the *American Intelligence*[363]. According to *Der Spiegel*, the “*American 007s”* had spied on *European* Diplomats, in *Washington* and *New York*. They had also intercepted *EU* computers and telephones, perhaps even those of the *EU* Leaders, in *Brussels*. Further more, a new "whistleblower", *Wayne Madsen*, a former Navy lieutenant who worked for the *NSA* since 1985, revealed to the *German* paper: “*Italy* but also *Germany*, *France* and other *European Countries* have secret agreements, in order to transfer personal data to the *United States*”[364].

On the other hand, *Le Monde* published the news that the *American NSA* had recorded up to 70.3 million telephone data, only from December 10 2012 to January 8 2013[365].

---

[363] Staff - "US-Geheimdienst: NSA führt Deutschland als Spionageziel", *Der Spiegel*, August 10, 2013.
[364] Barberis E. - “Il caso Datagate”, *La Stampa,* 2013.
[365] Follorou J. and Greenwald G. - "France in the NSA's crosshair: phone networks under surveillance", *Le Monde*, October 21, 2013.

44. Germany and *France*

The reactions of the *German* and the *French Heads of State*, respectively *Angela Merkel* and *François Hollande*, were similar. First of all, on July 1 2013, they both threatened to interrupt the trade negotiations of the *EU* with the *U.S.*[366]

Beyond this, in *France*, the *Minister of Foreign Affairs*, *Laurent Fabius*, convened the *U.S. Ambassador*, *Charles Rivkin*. For this reason, *Obama* had to call *Hollande*, in order to reassure him. "The *United States* started rethinking the way we gather information", was the *American President*'s justification[367]. *Fabius*, however, commented: "We were warned in June (about the *Program*) and we reacted strongly, but obviously we need to go further". "We must quickly assure that these practices aren't repeated", he added[368]. Further more, *Manuel Valls*, *France*'s *Interior Minister*, said the revelations were "shocking". "If an allied *Country* spies on *France* or spies on other *European Countries*, that's totally unacceptable", *Valls* told *Europe 1* radio, in October 2013[369].

At the same time, in *Germany*, Chancellor *Angela Merkel*, commenting the *Scandal* for *The Guardian* and other papers, stated: "If these reports are confirmed in the course of our investigations, we will be looking at an extremely serious incident. Using bugs to listen in on friends in our *Embassies* and *EU Representations* is not on. The cold war is over. There is no doubt whatsoever that the fight against terrorism is essential, and it needs to

---

[366] Bacchiddu P. - "Datagate, tutte le tappe dello scandalo, Le rivelazioni di Edward Snowden al Guardian, la difesa della Casa Bianca, le risposte carenti della Nsa, le reazioni degli alleati, la fuga in Russia del whistleblower. Nella nostra timeline tutte le tappe principali della vicenda", Timeline, *Espresso,* 2013.
[367] Follorou J. and Greenwald G. - "France in the NSA's crosshair: phone networks under surveillance", *Le Monde*, October 21, 2013.
[368] Staff - "France summons US ambassador over 'spying'", *Aljazeera*, October 21, 2013.
[369] Id.

harness intelligence about what happens online, but nor is there any doubt that things have to be kept proportionate. That is what guides *Germany* in talks with our partners"[370].

In fact, an essential cultural difference, that must be considered, is that the *German Chancellor*, and many other *German* citizens, grew up in communist *East Germany*, where the *Stasi*, the *State*'s secret police, use to spy on the citizens "against the regime". Therefore, while acknowledging the possible cooperation between *German* and foreign Intelligence Agencies, *Angela Merkel* refused to accept similar *privacy* breaches. "Like most *Germans*, I am well aware that other *Countries'* services have helped identify terrorist groups in *Germany* and prevent their attacks on a number of occasions. That said, the need to protect *privacy* also has to be respected alongside *security* interests. There has to be balance between the two", she concluded[371].

Even the *German Minister of Justice*, *Sabine Leutheusser-Schnarrenberger*, stated: "If these accusations are correct, this would be a catastrophe. The accusations against *Great Britain* sound like a *Hollywood* nightmare. The *European Institutions* should seek straight away to clarify the situation", she added, commenting also the *British Surveillance Program*[372].

Further more, a few months after the *Scandal*, finding out that also her personal phone had been wiretapped, the *German Chancellor* told the *American President* that "she unmistakably disapproves of and views as completely unacceptable such practices, if the indications are authenticated".

---

[370] Connolly K. - "Angela Merkel: NSA snooping claims 'extremely serious'", *The Guardian*, July 3, 2013.
[371] Id.
[372] Urquhart C. - "GCHQ monitoring described as a 'catastrophe' by German politicians", *The Guardian*, June 22, 2013.

“This would be a serious breach of confidence. Such practices have to be halted immediately", added *Steffen Seibert*, *Merkel*'s spokesman.

However, in response to these accusations, *Jay Carney*, the *White House Spokesman*, stated: "The *President* assured the *Chancellor* that the *United States* is not monitoring and will not monitor the communications of the *Chancellor*"[373]. Finally, once *Germany* pointed out the use of only the present and future tenses in the *American* justification, *Caitlin Hayden*, the *White House's National Security Council Spokeswoman*, repeated: "The *United States* is not monitoring and will not monitor the communications of *Chancellor Merkel*. Beyond that, I'm not in a position to comment publicly on every specific alleged intelligence activity". She contributed, therefore, to the *Germans*' doubts on the *U.S. Government*'s previous interceptions[374].

45. Italy, *UK* and *Spain*

Also in *Italy*, the reactions were bitter. Starting from the *President*'s, *Giorgio Napolitano*, who defined *Datagate* "a thorny affair that will have to find satisfactory explanations". After being reassured from *Obama*, however, the *Italian Prime Minister*, *Enrico Letta*, commented: "*Obama*'s words comfort me", and added: "I am confident that all explanations will be given and have no doubts", during an official visit to *Israel*. Also *Emma Bonino*, the *Italian Minister of Foreign Affairs*, moved in the same direction, expressing her confidence, on the fact that the *U.S.* would give *Italy* all the necessary information and appropriate assurances[375].

---

[373] Traynor I., Oltermann P. and Lewis P. - "Angela Merkel's call to Obama: are you bugging my mobile phone?", *The Guardian*, October 24, 2013.
[374] Id.
[375] Staff - "Bufera Datagate, Obama all'Europa: 'Vi forniremo tutte le informazioni'", *La Stampa*, July 1, 2013.

However, after the discovery of bedbugs in the *Italian Embassy* in *Washington*, the *Italian Minister of Defense*, *Mario Mauro*, declared to be "surprised" by the latest revelations about *Datagate*, and made it clear that the story was "to be verified". "If confirmed, though, the relations between *Italy* and the *USA* would be compromised, because among *NATO* allies, there is no need to spy", he added[376].

In the *United Kingdom*, instead, reactions were quite diverse. On one hand, Prime Minister *David Cameron*, as a historical ally of the *U.S.*, and sharing the shame for *UK*'s own *Surveillance Program*, defended both *Programs*, in the name of *National security*[377]. In fact, speaking for the first time publicly about the *Scandal*, he simply stated: "The plain fact is that what has happened has damaged *National security* and in many ways *The Guardian* themselves admitted that, when they agreed, when asked politely by my *National Security Adviser* and *Cabinet Secretary* to destroy the files they had, they went ahead and destroyed those files. So they know that what they're dealing with is dangerous for *National security*". *Cameron* went on, delegating the *House of Commons*, to analyze the possible law breaches of the parties involved in *Datagate*: "I think it's up to select *Committees* in this *House*, if they want to examine this issue, and make further recommendations"[378].

In the meantime, though, the *British Information Commissioner*, *Christopher Graham*, had asked his advisers to investigate, instead, the

---

[376] Id.
[377] Wintour P. - "Snowden leaks: David Cameron urges committee to investigate Guardian", *The Guardian*, October 16, 2013.
[378] Id.

consequences of *Edward Snowden*'s revelations on the *privacy* of *UK* citizens[379].

However, *Sir Andrew Parker*, the new *Director General* of the *British* counter-intelligence and security *Agency*, *MI5*, defended bluntly the counter terrorism *Programs*, in his first speech: "How the *UK* decides to respond to these (technological) developments will directly determine the level of *security* available against the threats we face"[380]. Further more, he added: "Retaining the capability to access such information is intrinsic to *MI5*'s ability to protect the *Country*. There are choices to be made, including about how and whether communications data is retained". "It is not, however, an option to disregard such shifts with an unspoken assumption that somehow *security* will anyway be sustained. It will not. We cannot work without tools", he finally concluded[381].

Also *Spain* reacted quite strongly to the *Scandal*. Surprisingly, though, the "*Centro Nacional de Inteligencia (CNI)*", the leading *Spanish* secret service *Agency*, had taken for granted that the powerful *American* electronic spy *Agency* (*NSA*) had intercepted massively private communications in *Spain*. But it did not imagine that it had specifically intercepted *Spanish* politicians[382].

After *Snowden's* leak, in fact, the *Spanish Minister of Defense*, *Pedro Morenés*, stated emphatically: "They have not spied on me and, I think, in general, neither on others (*Spanish Authorities*)". Beyond this, apparently, he

---

[379] Travis A. - "UK information commissioner to examine Snowden disclosures impact", *The Guardian*, September 19, 2013.
[380] Hopkins N. - "MI5 chief: GCHQ surveillance plays vital role in fight against terrorism", *The Guardian*, October 9, 2013.
[381] Id.
[382] González M. - "Washington controló millones de llamadas y espió a políticos en España", *El Pais*, October 24, 2013.

confessed: "What matters to me is the mobile of *Rajoy* (the *Spanish President*)", after finding out that the mobile of *Chancellor Angela Merkel* had been intercepted[383].

However, in the following days, the *American Ambassador* was summoned in *Madrid*, for details on the *NSA* wiretapping, by the *Spanish Minister for European Affairs*, *Iñigo Méndez de Vigo*. *De Vigo* called "inappropriate and unacceptable" the operations of the *U.S. Government Agency*, pointing out "the importance of preserving the trust governing bilateral relations and to know the scope of practices which, if true, are inappropriate and unacceptable among partners and friendly *Countries*". Further more, *Méndez de Vigo* has requested the *United States* to maintain "the necessary balance that must be maintained between all *security* systems, *privacy* protection and communications' *privacy*, as the *Spanish* law clearly states"[384].

Finally, the *Spanish Minister of Foreign Affairs*, *José Manuel García-Margallo*, repeated, once and for all, *Spain's* position on the *Scandal*: "if the *NSA* activities are confirmed, they threat to ruin the climate of trust between the two *Countries* (*Spain* and *U.S.*)"[385].

46. The *EU*'s Reaction

Beyond the reactions of individual *Member States*' Leaders and Ministers, the *European Union* reacted as a whole. Since the *Scandal*, in fact, it has been protesting strongly against *Washington*, demanding explanations,

---

[383] Id.
[384] Romero A. - "Margallo: si se confirma el espionaje, podría suponer 'ruptura de confianza' entre España y EEUU", *El Mundo*, October 28, 2013.
[385] Id.

and threatening to break off the negotiations for a transatlantic free trade agreement.

For this reason, the *European Diplomatic Service* had "made contact with the *American* authorities in *Washington* and *Brussels* for urgent clarification on the truthfulness of the facts", confirmed the *EU High Representative for Foreign Policy*, *Catherine Ashton*. "As a matter of concern, we will not make any further comment at this stage, until there is greater clarity on the subject", she added[386].

The reply of the *U.S. Secretary of State*, *John Kerry*, was that the search for information on other *Countries* was not "unusual". *Kerry*, though, at the time in *Brunei*, declined to comment directly the controversy, sparked by the *Datagate Scandal*. "*Ashton* discussed (the theme) with me today, and we decided to stay in touch. I agreed to try to find out exactly what it is and I will share my conclusions", *Kerry* stated, after meeting with the *Head of EU Diplomacy*. "I will say that every *Country* in the World, engaged in International affairs and *National security*, undertakes many activities, in order to protect its *National security*, and gathers any information that could help. All I know is that this is not unusual for many *Countries*", he finally repeated[387].

At the same time, however, the *Permanent Representative of Lithuania*, who had just undertaken the *EU* presidency, at the time, recalled the *United States* to be "a political and economical ally". "They should make this situation clear, we need an official answers", he then added, though[388]. "Enough is enough: between friends, there must be trust. It's been

---

[386] Staff - "Datagate, gli Usa spiavano anche l'Italia. Reazione Ue: a rischio negoziati commerciali", *First Online*, July 1, 2013.
[387] Staff - "Datagate, caos e reazioni in Ue", *Il Secolo XIX*, July 1, 2013.
[388] Id.

compromised. We expect answers by the *Americans*, quickly" had also commented the *EU Internal Market Commissioner*, *Michel Barnier*[389].

Further more, the *Brussels Summit* of *EU Heads of State*, in October 2013, literally shifted the topics of its agenda, because of the shock of the revelations on the *American Surveillance Program*. In fact, what was supposed to be a *European Summit* dedicated to the issues of immigration, after the tragedy of *Lampedusa* (*Italy*), and to the economic routine, in particular to the progress of the *European Banking Union*, was literally hit by the growing tensions for the *Scandal*, triggered by the *U.S.* monitoring their allied (*EU Member*) *States*[390].

Consequently, at the *Brussels Summit*, the *Europeans* were divided between blocking or not the *Draft Law* on *Data Protection*, submitted several months earlier by the *European Commission*, which we introduced in *Chapter II*. Following the *Datagate Scandal*, in fact, the *Commission* wanted the large Internet companies to obtain the prior consent of the people, for the use of their personal data, under the threat of sanctions[391].

Beyond this, the *EU Justice Commissioner*, *Viviane Reding*, called for the *Data Protection Reform* to be adopted by spring 2014. In fact, referring to the *Datagate Scandal*, she stated: "the time has come for *Europe* to give the *Americans* a strong and unequivocal answer". "Data protection must apply to citizens' emails, as well as to *Angela Merkel*'s mobile. Now it is no longer the time to simply make statements, we must act at this *Summit*", she added. And, finally, she concluded: "This will allow us to negotiate with the *United*

---

[389] Staff - "Datagate, spiati 35 leader mondiali. La Ue: risposta forte agli Stati Uniti", *Il Messaggero*, October 24, 2013.
[390] Cascioli R. - "Il Datagate stravolge l'agenda. Proposto il blocco del negoziato commerciale Usa-Ue", *Europa Quotidiano*, October 25, 2013.
[391] Id.

States with a strong and unique voice", referring to the divisions within the *EU*, that had slowed down for months the process, to establish an adjourned policy, on *privacy* and personal data respect standards.

In the same direction, the *EU President*, *Herman van Rompuy*, stated: "In the conclusions of the *EU Summit's Draft*, the Leaders discussed today, there is a reference to the need to adopt the *Directive* on *Data Protection* next year, because it is important to restore confidence"[392].

However, also the *European Parliament*, on its behalf, had reacted strongly. In fact, it approved a *Resolution*, passed by a large majority, asking the *Commission* to suspend one of the most important agreements between the *EU* and the *U.S.*, on the fight against terrorism. It regarded the *Swift Program*, through which all the movements of capital from one side of the *Atlantic Ocean* to the other could be traced, for the data to be then stored in a giant database. The *Resolution* was not binding, however[393].

Beyond this, the *President of the European Parliament*, *Martin Schulz*, had formally requested the suspension of the ongoing negotiations to reach a free trade agreement between the *EU* and the *U.S*[394]. The *European Commission*, though, ensured the *Parliament* and its *President* that it would take concrete steps, asking the *Washington Authorities* for further explanations, and also for "written" information[395].

From then onwards, given the historical bonds between most of the *EU Countries* and the *U.S.*, and, mostly, given the reassurances of the *U.S. President* and *Congress*, the Transatlantic Alliances and Cooperation

---

[392] Id.
[393] Id.
[394] Cascioli R. - "Il Datagate stravolge l'agenda. Proposto il blocco del negoziato commerciale Usa-Ue", *Europa Quotidiano*, October 25, 2013.
[395] Staff - "Datagate, spiati 35 leader mondiali. La Ue: risposta forte agli Stati Uniti", *Il Messaggero*, October 24, 2013.

Programs have been safeguarded. However, this *Scandal* has definitely diminished the climate of reciprocal trust between the *EU* and the *U.S.*

47. Consequences

After reviewing the reactions from both sides of the *Atlantic*, it is not hard to understand that this *Scandal* has, for a vast majority, breached the *boundaries between individual privacy and National security*, wherever those are. We have already presented, though, in the previous *Chapter*, the *EU*'s project of a more accurate *Data Protection Regulation*. Beyond this, we just mentioned that this *Reform* will obviously take into account the *Scandal*-related problems, and hopefully be effective by the end of 2014.

Not surprisingly, though, also the *United States* have taken action on the matter, beyond the statements of *Kerry* and *Obama*. Last June, in fact, the *U.S. Congress* voted in favor of an *Amendment* to the *Defense Appropriations Bill*, that limits the *NSA*'s spying ability.

The *Amendment* was introduced by the Republicans *James Sensenbrenner*, *Thomas Massie* and *Zoe Lofgren*, and won the approval, in the *House of Representatives*, by an overwhelming majority: 293 in favor and 123 against. The *Measure*, which is not yet *Law*, would put a stop to mass surveillance of the *NSA*. In particular, the *Proposal* regards the 2015 *Defense Appropriations*, and has the goal to reduce specifically the *Agency's* budget, used so far to intercept *American* citizens, and to convince businesses and organizations to add backdoors in encryption products, giving *NSA* the ability to access private information[396].

On the night of the *Bill*'s approval by the *House*, in fact, *Mark Rumold*, *Staff Attorney* for the *Electronic Frontier Foundation*, stated: "Tonight, the

[396] Dotti G. - "Congresso Usa, sì al taglio dei fondi per lo spionaggio dell'Nsa", *Wired*, June 20, 2014.

House of Representatives took an important first step in reining in the *NSA*. The *House* voted overwhelmingly to cut funding for two of the *NSA*'s invasive surveillance practices: the warrantless searching of *Americans'* International communications, and the practice of requiring companies to install vulnerabilities in communications products or services. We applaud the *House* for taking this important first step, and we look forward to other elected officials standing up for our *right to privacy*"[397].

The *U.S. Senate*, though, must still approve the *Bill's Draft*, with the proposed *Amendments*, first, and so does President *Obama*, afterwards. Only then will it become *Law*, in all respects. However, regardless of the outcome, the vote of last June clearly shows a great disapproval of the *NSA Program*, from the *U.S. Congress*. By the way, this could be only the first of a series of *Amendment*s, in the same direction[398].

Further more, on July 17 2014, *U.S.* Senator *Barbara A. Mikulski*, *Chairwoman* of the *Senate Appropriations Committee*, announced that "the *Full Committee* has approved the fiscal year 2015 *Department of Defense Appropriations Bill* unanimously by voice vote". "The measure, therefore, will be reported to the full *Senate* for consideration", she added[399].

Beyond this, on August 10, the *U.S. Senate Majority Leader*, *Harry Reid*, has included the fiscal 2015 *Defense Authorization Bill* on his to-do list for September. However, the *Senate*'s busy schedule may postpone the debate on the legislation. In fact, given the limited floor time available, and the number of *Amendments* filed on the 2015 *Defense Policy Bill*, it could take

---

[397] Reitman R. - "House Has Passed an Amendment to Cut NSA Search Funding", *Electronic Frontier Foundation*, June 20, 2014.
[398] Dotti G. - "Congresso Usa, sì al taglio dei fondi per lo spionaggio dell'Nsa", *Wired*, June 20, 2014.
[399] Morris V. - "Committee Approves FY 2015 Department of Defense Appropriations Bill", *U.S. Senate Committee on Appropriations*, July 17, 2014.

quite some time for the *Senate* to actually vote it. Actually, 141 *Amendments* have been filed already, so far, but the number will certainly rise, before the *Bill* goes to the floor[400]. Finally, *Carl Levin*, *Chairman* of the *Senate Armed Services Committee*, hopes that the *Senate* shall vote a few *Amendments* only, avoiding the problems occurred for the *2014 Defense Bill's* approval[401].

Hopefully, therefore, also the *U.S. Defense Appropriations Bill* should be *Law* by the end of this year, as the new *EU Data Protection Regulation*. However, as mentioned in *Chapter I*, it will take time for the *U.S.* to adopt a new and unitary Federal data protection policy, in light of its history and diverse cultural orientation. Having analyzed the different *reactions* to a common *Scandal*, involving *Individual privacy* and *National security*, it is time for us to finally compare the *American* and the *European boundaries*, between those.

[400] Staff - "Prospects Remain Uncertain for Senate to Debate Authorization Bill Next Month", *Association of Defense Communities*, August 10, 2014.
[401] Id.

Conclusions

This analysis of the *U.S.* and *EU privacy-security* policies and limits, therefore, has made their differences clear. In fact, while *EU* law, no matter its ultra-national value, appears to have an organic structure, *U.S.* law, instead, seems deeply fragmented among its 50 *States'* individual legislations. Further more, laws in *Europe* seem particularly inspired by a common constitutional tradition of fundamental rights, differently to what often occurs to the laws in the *United States*.

The *European* model of *privacy*, in fact, has expressly incorporated the core values of the *Convention for the Protection of Human Rights and Fundamental Freedoms* (1950)[402]. Therefore, the *EU*'s *Directives* strongly limit the *European Legislator's National security*-related provisions, in the name of personal data protection, unlike the latest *U.S. Emergency Legislation,* which appears to confer the *American Executive Branch* "almost unlimited" powers.

Moreover, beyond the contrasts of the *European Union* and the *United States* as prevalently Civil law and Common law legal orders, and their consequent different legislative and jurisprudential models, a further difference among them is the kind of protection they offer. On one hand, *European* law grants a "general protection" of *privacy*, which includes all its possible breaches and *security*-related exemptions, while, on the other hand, *American* law grants a "sectorial protection" of *privacy*, specifically connected to *identity theft*, rather than to *video voyeurism*, etc.[403].

The issues of *United States' privacy* policies, therefore, are mainly due to the lack of Federal rules governing the matter, at a constitutional level. In

---

[402] See *Paragraph 18*.
[403] See *Paragraph 6*.

fact, the *Datagate Scandal* has contributed to highlight the structural limits of the *U.S.'* "exclusively-sectorial" approach, especially in its *Emergency Legislation*, introduced since the *Patriot Act*[404], and reiterated with the recent *PRISM Program*[405].

The reason why the *United States* have never approved a strong Federal discipline on the matter, as the legislative model adopted in *Europe*, though, is probably not "only" due to the fact that they have not recognized, yet, the role that *privacy* should have among the *Individual*'s fundamental rights. Beyond this, in fact, another (and maybe greater) reason is surely the recent history of terrorist attacks in the *U.S.* Territory, and the constant threats its boarders have been facing since the *9/11 Attack*.

At least recently, therefore, these threats have been definitely upholding the *Government*'s policy of subordinating any other right to the *Nation*'s *security*. This, of course, contributes to an often-insufficient protection of data protection rights, and, more specifically, to the absence of a balance between the respect of *Individual privacy* and the needs of *National security*.

However, this *U.S.* - *EU* policies' analysis has also revealed the *European Union*'s constant attitude, certainly pre-existing to the recent *Datagate Scandal*, to adopt and implement a gradually better *privacy* legislation. Further more, this process has always occurred in accordance with the *EU Member States' security* standards, so far, but has also been taking into account the needs for progress of the *Individuals*' rights, at the same time.

---

404 See *Paragraph 11*.
405 See *Paragraph 39*.

This was an absolute surprise for me. Actually, while approaching the subject, I believed it impossible that a *Union* of 28 different *National States*, and respective legal cultures, could have, at least in some areas of law, stricter and better-unified policies than one *Sovereign Nation*, no matter its 50 *States* (culturally different, but definitely not as much as *Europe*'s).

What I understood, though, is that the system of "check and balances", that allows the three branches of power to supervise each other, in the *U.S.*, has been someway exported to the *EU*, allowing individual *Governments* to check, balance, and also to "push" each other towards progressive policies. As already mentioned, the latter also reflect the common, and therefore stronger, constitutional traditions. A recent example of this trend is *Germany*'s insistence for the public and private sectors' equivalent *privacy* standards, to be included in the *EU Commission*'s proposed *Regulation*[406], in order for *Berlin's Government* to grant its vote[407]. *Germany*'s attitude is a consequence of its will to adopt in the rest of the *Union* its already-effective National *privacy* standards.

Beyond this, the *EU*'s constant progress, as a *Union*, is demonstrated by its historically quick substitutions and/or amendments of fundamental *Data Protection Directives* (1995, 2002, 2006, 2009), and by its will to keep improving (2012 *Draft*, to be implemented by the end of 2014), evidenced in *Chapter II*[408]. Compared to the *U.S. Privacy Act* (1974)[409], to the *American Government*'s difficulties to properly replace it, and to the limits of the *U.S.*

---

406 "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Brussels, 25.1.2012 com (2012) 11 final 2012/0011 (cod), *European Commission*.
407 See *Paragraph 35*.
408 See *Paragraphs 24, 32, 33, 34* and *35*.
409 *Privacy* Act, Public Law 93-579, 88 Stat. 1897, in 5 U.S.C. n 552, 1974.

Federation's 50 individual *States*' legislations, therefore, the *EU* can definitely be considered a model for *privacy* standards. Even the *American Civil Liberties Union* has underlined this, at the beginning of 2013: "unlike the *United States*, *Europe* has a set of basic rules and institutions in place to protect *individuals*' *privacy*, and is trying to update its existing rules and institutions for the digital age"[410].

However, we need to point out that also the *European Union*'s system has its limits, of course. For example, as a non-Federation, comprising so many different *National* policies, it has to grant its *Member States* partial autonomy, for the application of its *Directives* in their Territories. In fact, in the *privacy* area, for example, the *EU* legal system has left a wide range of discretion to its *Member States*, in order to obtain the results required by the *Data Protection Directive*, and without prejudice to the essential purpose of achieving a common specific goal. Consequently, it sometimes has problems to obtain uniform standards in the 28 separate legislations, fast enough.

Further more, to evaluate correctly the *U.S.-EU* different *privacy-security* standards, we need to keep in mind their crucial historical differences, such as the already mentioned[411] former *European* dictatorships (*Mussolini's* in *Italy*, *Hitler's* in *Germany*, *Franco's* in *Spain*, etc.). There is no doubt, in fact, that the current *privacy-security boundary* in *Europe* is also a consequence of such a repressive history, during which the *Nation* had prevailed on the *Individual*, in all areas. From the fall of these *Regimes*, and especially since the reunification of *Germany*, therefore, the *European Union* citizens, and their democratically elected Representatives, have been literally

---

[410] Stanley J. - "US Government Busy in Europe Defending Interests of Advertisers, Security Agencies, But Not Americans' Privacy", *American Civil Liberties Union*, January 22, 2013.
[411] See *Paragraph 44*.

"requiring" *Individual privacy*, and are culturally less keen than the *Americans* to give any part of it up, even if "in the name of *National security*".

Having said this, the public opinion and some of the most important associations for the protection of civil rights, in the *United States*, have served well their task of "watch dogs", with respect to the decisions taken by the *U.S. Government*, lately. In fact, the control of the constitutional legitimacy of laws and a large number of the *Supreme Court*'s judgments has already severely reduced the harvest of unfair provisions.

Hopefully, though, the recent *European Authorities'* critics, and the ongoing battles, in the *Courts* (*ACLU vs. NSA*[412]) and in the *Congress* (2015 *Defense Appropriations Budget*[413]), due to *Datagate*, will contribute to limit further the *U.S. Government*'s *privacy*-breaching powers, in order to avoid other violations of the *American* and *European* citizens' homes, or "castles"[414], in the future.

Finally, beyond the *EU* and the *U.S.* legal policies, we must keep in mind our own self-exposure to the digital world. In fact, provided a development of further legal safeguards by our *Governments*, the cause of an insufficient data protection, in the end, is often the impatient analysis of the *privacy agreements* of our social networks, email accounts, and web search engines. Personally, my recent *privacy-security* related studies have opened my eyes on the many risks I have been taking, while surfing the web, as many other users. However, as for all the areas of law, a better knowledge of the policies, and a greater caution in our actions, may help us protect our

---

[412] See *Paragraph 42*.
[413] See *Paragraph 47*.
[414] Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, page 220.

"castles", and set, once and for all, clear *boundaries between Individual privacy and National security*.

Sources

Bibliography

Abernathy F. – *Defining "Privacy": The Power of Culture in a Digital Age,* in Privacy: Altre Voci (Ugo Pagallo ed., 2005).

Allen C. K. - *Law in the Making*, Third edition, Oxford: Clarendon Press, 1939.

Bacchiddu P. - "Datagate, tutte le tappe dello scandalo, Le rivelazioni di Edward Snowden al Guardian, la difesa della Casa Bianca, le risposte carenti della Nsa, le reazioni degli alleati, la fuga in Russia del whistleblower. Nella nostra timeline tutte le tappe principali della vicenda", Timeline, *Espresso,* 2013.

Barberis E. - "Il caso Datagate", *La Stampa,* 2013.

Bassu C. - "La legislazione antiterrorismo e la limitazione della libertà personale in Canada e negli Stati Uniti", in Groppi T. - *Democrazia e terrorismo. Diritti fondamentali e sicurezza dopo l'11 settembre 2001*, Editoriale Scientifica, Napoli, 2006.

Beck G. – "The German Constitutional Court versus the EU: self assertion in theory and submission in practice – Euro Aid and Financial Guarantees. Part 3", *Eutopia Law*, October 26, 2011.

Bilancia P. and Pizzetti F.G. - *Aspetti e problemi del costituzionalismo multilivello*, Giuffrè, Milano, 2004.

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

Branigan T. and Elder M. - "Edward Snowden leaves Hong Kong for Moscow, NSA whistleblower left on Aeroflot flight to Moscow, Hong Kong government confirms, two days after US charged him with espionage", *The Guardian*, June 23, 2013.

Braun S., Flaherty A., Gillum J. and Apuzzo M. - "Secret to PRISM Program: Even Bigger Data Seizures", *Associated Press*, June 15, 2013.

Bump P. - "The UK Tempora Program Captures Vast Amounts of Data — and Shares with NSA", *The Wire*, June 21, 2013.

Cascioli R. - "Il Datagate stravolge l'agenda. Proposto il blocco del negoziato commerciale Usa-Ue", *Europa Quotidiano*, October 25, 2013.

Cassese S. - *La crisi dello stato*, Laterza, Roma-Bari, 2002.

Chappell B. - "NSA Reportedly Mines Servers of US Internet Firms for Data". *The Two-Way (blog of NPR)*, June 6, 2013.

Chebel d'Appollonia A. and Reich S. – *Immigration, Integration, and Security, America and Europe in Comparative Perspective*, University of Pittsburgh Press, Pittsburgh PA, 2008.

Coing H. - *Von Bologna bis Brussels: Europäische Gemeinsamkeit, Gegenwart und Zukunft*, Kölner Juristische Gesellschaft, IX, Bergish Gladbach-Köln, 1989.

Connolly K. - "Angela Merkel: NSA snooping claims 'extremely serious'", *The Guardian*, July 3, 2013.

Cooper D., Tielemans H. and Young M. - "International Data Privacy Update November 2009," *ADVISORY - Covington & Burling LLP*, November 20, 2009.

Dicosola M. – "The Interaction between EU and National Law in Italy. The Theory of 'limits' and 'counter-limits'", *Co.Co.A. Comparing Constitutional Adjudication A Summer School on Comparative Interpretation of European Constitutional Jurisprudence*, University of Trento, Department of Legal Sciences Faculty of Law, 2nd Edition - 2007.

Dotti G. - "Congresso Usa, sì al taglio dei fondi per lo spionaggio dell'Nsa", *Wired*, June 20, 2014.

Douma W.T. - "European Environmental Law after Lisbon: an introduction", *Asser Institute, Center for International & European Law*.

Doyle J. and Greenwood C. - "Guardian may face terror charges over stolen secrets: Met Deputy Commissioner confirms she is investigating whether newspaper broke the law", *Daily Mail*, December 3, 2013.

Etzioni A. - *How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism*, Taylor & Francis, 2004.

Fantz A., Black P. and Martinez M. - "Snowden out of airport, still in Moscow", *CNN*, August 2, 2013.

Follorou J. and Greenwald G. - "France in the NSA's crosshair : phone networks under surveillance", *Le Monde*, October 21, 2013.

Freedman W. – *The Right to Privacy in the Computer Age*, Quorum Books, New York, NY, 1987.

Gellman B. - "Edward Snowden, after months of NSA revelations, says his mission's accomplished", *The Washington Post*, December 23, 2013.

Gellman B. and Soltani A. - "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". *The Washington Post*, October 30, 2013.

Gellman B. and Poitras L. - "US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program", *The Washington Post*, June 6, 2013.

Gentili G. - "Stati Uniti. Estesa sino al 2015 l'efficacia del Patriot Act tra crescenti critiche circa la possibile violazione di diritti fondamentali garantiti dalla Costituzione", *DPCE online,* Numero 3, 2011.

Glenn R. A. and D.G. Jr. Stephenson - *The Right to Privacy: Rights and Liberties Under the Law*, ABC-CLIO, 2003.

González M. - "Washington controló millones de llamadas y espió a políticos en España", *El Pais*, October 24, 2013.

Gorman S. and Valentiono-Devries J. - "New Details Show Broader NSA Surveillance Reach - Programs Cover 75% of Nation's Traffic, Can Snare Emails", *The Wall Street Journal*, August 20, 2013.

Greenwald G. - "NSA collecting phone records of millions of Verizon customers daily, Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama", *The Guardian*, June 6, 2013.

Greenwald G. and MacAskill E. - "NSA Prism program taps in to user data of Apple, Google and others, Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook, Companies deny any knowledge of program in operation since 2007", *The Guardian*, June 7, 2013.

Greenwald G., MacAskill E. and Poitras L. - "Edward Snowden: the whistleblower behind the NSA surveillance revelations, The 29-year-old source behind the biggest intelligence leak in the NSA's history explains his motives, his uncertain future and why he never intended on hiding in the shadows", Glenn Greenwald, Ewen MacAskill and Laura in Hong Kong, *The Guardian*, June 10, 2013.

Harris L. and Westin A. F. – *The Dimensions of Privacy. A National Opinion Research Survey of Attitudes toward Privacy*, Garland Publishing, New York, NY, 1981.

Hendricks E., Hayden T. and Novik J. – *Your Right to Privacy. A Basic Guide to Legal Rights in an Information Society*, Southern Illinois University Press, Carbondale, IL, 1990

Holtzman D.H - *Privacy Lost: How Technology Is Endangering Your Privacy*, San Francisco: Jossey-Bass, 2006.

Hopkins N. - "MI5 chief: GCHQ surveillance plays vital role in fight against terrorism", *The Guardian*, October 9, 2013.

Lake E. - "Greenwald: Snowden's Files Are Out There if 'Anything Happens' to Him", Politics, *The Daily Beast*, June 25, 2013.

Lally K. and Englund W. - "Putin: No grounds to extradite Snowden", *The Washington Post*, June 25, 2013

Lavender P. - "Edward Snowden Receives Sam Adams Award", *Huffington Post*, December 10, 2013.

Lugaresi N. – *Internet, Privacy e Pubblici Poteri Negli Stati Uniti*, Seminario Giuridico della Università di Bologna, Milano, Giuffrè Editore, 2000.

Luhn A. and Tran M. - "Edward Snowden given permission to stay in Russia for three more years", *The Guardian*, August 7, 2014.

Macaskill E., Dance G., Cage F. and Chen G. - "NSA Files: Decoded, What the revelations mean for you.", *The Guardian*, November 1, 2013.

MacAskill E., Davies N., Hopkins N., Borger J. and Ball J. - "GCHQ intercepted foreign politicians' communications at G20 summits", *The Guardian*, June 17, 2013.

MacAskill E., Borger J., Hopkins N., Davies N. and Ball J. - "GCHQ taps fibre-optic cables for secret access to world's communications, Exclusive: British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls, and shares

them with NSA, latest documents from Edward Snowden reveal", *The Guardian*, June 21, 2013.

MacCormick N. - *Questioning Sovereignty. Law, State, and Nation in the European Commonwealth*, Oxford University Press, Oxford, 1999.

Markesinis B.S. and Deakin S.F. - *Tort Law*, 4th Edition, Clarendon Press, 1999.

Maurizi S. - "Datagate. Bonino, perché non risponde?", *Espresso*, July 9, 2013.

Miranda R. - "Datagate, la furbetta strategia dell'Europa", *Formiche*, October 29, 2013.

Moore A.D. – *Privacy Rights, Moral and Legal Foundations*, The Pennsylvania State University Press, University Park, Pennsylvania, 2010.

Morris V. - "Committee Approves FY 2015 Department of Defense Appropriations Bill", *U.S. Senate Committee on Appropriations*, July 17, 2014.

Nakashima E. and Del Quentin W. - "Report Says TSA Violated Privacy Law", *Washington Post,* December 22, 2006.

Pagallo U. - *La Tutela della Privacy Negli Stati Uniti D'America e in Europa*, Giuffrè Editore, 2008.

Pagallo U. - *Teoria giuridica della complessità. Dalla 'polis primitiva' di Socrate ai 'mondi piccoli' dell'informatica. Un approccio evolutivo*, Giappichelli, 2006.

Pagallo U. and Gentile F. - *Testi e contesti dell'ordinamento giuridico: Cinque studi di teoria generale del diritto*, Padova, CEDAM, 1998.

Pernice I. - "Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitutionalism in Making Revisited?", *Common Market Law Review*, 1999.

Pinelli C. - *Il momento della scrittura. Contributo al dibattito sulla Costituzione europea*, Il Mulino, Bologna, 2002.

Prosser W. L. – "Privacy, a legal analysis", *California Law Review*, n.48, 1960.

Prosser W.L. and Wade J. W. - "Restatement of the Law, Second, Torts", *American Law Institute*, 1961.

Puliafito A. - "Datagate: il Washington Post e il New York Times contro Obama", *Polis Blog*, August 10, 2013.

Regan P. M. – *Legislating Privacy: Technology, Social Values, and Public Policy*, The University of North Carolina Press, Chapel Hill, NC, 1995.

Reitman R. - "House Has Passed an Amendment to Cut NSA Search Funding", *Electronic Frontier Foundation*, June 20, 2014.

Ripsman N.M. and Paul T.V. – *Globalization and the National Security State*, Oxford University Press, Inc., 2010.

Roberts D. - "NSA mass collection of phone data is legal, federal judge rules", *The Guardian*, December 27, 2013.

Roberts D., Ackerman S. and Travis A. - "NSA surveillance: anger mounts in Congress at 'spying on Americans'", *The Guardian*, June 12, 2013.

Rodotà S. - *Intervista su privacy e libertà*, a cura di Paolo Conti, Editori Laterza, Roma-Bari, 2005.

Romero A. - "Margallo: si se confirma el espionaje, podría suponer 'ruptura de confianza' entre España y EEUU", *El Mundo*, October 28, 2013.

Rosenberg J.M. – *The Death of Privacy*, Random House, New York, NY, 1969.

Russo S. and Sciuto A. - *Habeas Data e Informatica*, Giuffrè Editore, 2011.

Schilling T. - "The Autonomy of the Community Legal Order – An Analysis of Possible Foundations", *Harvard International Law Review*, 37 Harvard International Law Journal 389, Spring, 1996.

Schwartz P. M. and Reidenberg J. R. – *Data Privacy Law. A Study of United States Data Protection*, Michie Law Publishers, Charlottesville, VA, 1996.

Shubber K. - "A simple guide to GCHQ's internet surveillance programme Tempora", Politics, *Wired UK*, June 24, 2013.

Smith H. J. – *Managing Privacy. Information Technology and Corporate America*, The University of North Carolina Press, Chapel Hill, NC, 1994.

Solove D., Rotenberg M. and Schwartz P.M. – *Privacy, Information and Technology*, Aspen, New York, 2006.

Staff - "About the ACLU", *American Civil Liberties Union Website*.

Staff - "ACLU v. Clapper – Challenge to NSA Mass Call-Tracking Program", *American Civil Liberties Union Website*.

Staff - "Bufera Datagate, Obama all'Europa: 'Vi forniremo tutte le informazioni'", *La Stampa*, July 1, 2013.

Staff - "Datagate, caos e reazioni in Ue", *Il Secolo XIX*, July 1, 2013.

Staff - "Datagate, gli Usa spiavano anche l'Italia. Reazione Ue: a rischio negoziati commerciali", *First Online*, July 1, 2013.

Staff - "Datagate, 'Sbaglio spiare i leader'", *TGCOM24*, October 28, 2013.

Staff - "Datagate, spiati 35 leader mondiali. La Ue: risposta forte agli Stati Uniti", *Il Messaggero*, October 24, 2013.

Staff - "France summons US ambassador over 'spying'", *Aljazeera*, October 21, 2013.

Staff - "MATRIX: Myths and Reality", *American Civil Liberties Union*, February 10, 2004.

Staff - "Obama defends Internet surveillance programs - video", *Reuters*, Saturday 8 June 2013.

Staff - "Prospects Remain Uncertain for Senate to Debate Authorization Bill Next Month", *Association of Defense Communities*, August 10, 2014.

Staff - "US-Geheimdienst: NSA führt Deutschland als Spionageziel", *Der Spiegel*, August 10, 2013.

Stanley J. - "US Government Busy in Europe Defending Interests of Advertisers, Security Agencies, But Not Americans' Privacy", *American Civil Liberties Union*, January 22, 2013.

Timberg C. - "U.S. threatened massive fine to force Yahoo to release data", *The Washington Post*, September 11, 2014.

Travis A. - "UK information commissioner to examine Snowden disclosures impact", *The Guardian*, September 19, 2013.

Traynor I., Oltermann P. and Lewis P. - "Angela Merkel's call to Obama: are you bugging my mobile phone?", *The Guardian*, October 24, 2013.

Urquhart C. - "GCHQ monitoring described as a 'catastrophe' by German politicians", *The Guardian*, June 22, 2013.

Valentiono-Devries J. and Gorman S. - "What You Need to Know on New Details of NSA Spying", *The Wall Street Journal*, August 20, 2013.

Wade D. - *Virginia Law Weekly Dicta*, October 8, 1964.

Warren Samuel and Brandeis Louis D. - "The Right To Privacy", *Harvard Law Review* (Vol. IV, No. 5), 1890, pages 193 - 220.

Weiler J.H.H. - *The Constitution of Europe. "Do the New Clothes Have an Emperor?" and Other Essays on European Integration*, Cambridge University Press, Cambridge, 1999.

Wintour P. - "Snowden leaks: David Cameron urges committee to investigate Guardian", *The Guardian*, October 16, 2013.

Whittaker Z. - "PRISM: Here's How the NSA Wiretapped the Internet", *ZDNet*, June 8, 2013.

Zakaria T. and Charles D. - "NSA chief defends agency amid U.S. spy rift with Europe", *Reuters*, October 29, 2013.

U.S. Legislation

Bank Secrecy Act, Public Law 91-508, 1970.

Californian Code on Business and Professions, § 17538.4, 2003.

Children's Online Privacy Protection Act (COPPA), Public Law 105-277, div. C, title XIII, 112 Stat. 2681-728 (15 U.S.C. 6501 et seq.), 1998.

Communications Assistance for Law Enforcement Act, Public Law 103-414, 108 Stat. 4279, 1994.

Computer Matching and Privacy Protection Act, Public Law 100-503, 5 U.S.C. § 552a, 1988.

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) ACT, Public Law 113-121, 15 U.S. Code § 7701, 2003.

Driver's Privacy Protection Act (DPPA), Chapter 123 of Title 18 of the United States Code, 1994.

Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510-22, 1986.

First Amendment, U.S. Constitution.

Foreign Intelligence Surveillance Act (FISA), Public Law 95–511, 92 Stat. 1783, 50 U.S.C., 1978.

Fourth Amendment, U.S. Constitution.

Fourteenth Amendment, U.S. Constitution.

Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, 1966.

Genetics Information Non-Discrimination Act (*GINA*), Public Law 110–233, 122 Stat. 881, 2008.

Health Insurance Portability and Accountability Act (HIPAA), Public Law 104–191, 110 Stat. 1936, 1996.

Identity Theft and Assumption Deterrence Act, Public Law 105–318, 112 STAT. 3007, 1998.

N.Y. Civ. Rights Law §§ 50-51.

Omnibus Crime Control and Safe Streets Act, Public Law 90–351, 82 Stat. 197, enacted on June 19, 1968, codified at 42 U.S.C. § 3711.

PATRIOT Sunsets Extension Act, S. 1038 (112th), 2011.

Personal Responsibility and Work Opportunity Reconciliation Act (PRWOR), Public Law 104-193, 1996.

Privacy Act, Public Law 93-579, 88 Stat. 1897, in 5 U.S.C. n 552, 1974.

Secure Flight Program, Transportation Security Administration.

USA PATRIOT Act, Public Law 107-56, 2001.

USA PATRIOT Act Additional Reauthorizing Amendments Act, Public Law 109–178, 2006.

USA PATRIOT Improvement and Reauthorization Act, Public Law 109–177, 2005.

Video Privacy Protection Act (VPPA), Public Law 100–618, 1998.

Video Voyeurism Prevention Act, Public Law 108-495, 2004.

U.S. Case Law

Bowers v. Hardwick, 478 U.S. 186, 1986.

Ettore vs. Philco Television Broadcasting Co., 229 F.2d 481 (3rd Cir. 1956).

Frisby v. Schultz, 487 U.S. 474, 1988.

Griswold v. Connecticut, 381 U.S. 479, 1965.

Katz. v. United States, 389 U.S. 347, 1967.

Lawrence v. Texas, 539 U.S. 558, 2003.

Lochner v. New York, 198 U.S. 405, 1905.

McIntyre v. Ohio Board of Elections, 514 U.S. 334, 1995.

Meyer v. Nebraska, 262 U.S. 390, 1923.

NAACP v. Alabama, 357 U.S. 449, 1958.

New York Times Co. v. Sullivan, 376 U.S. 254, 1964.

Pavesich v. New England Life Insurance CO., 50 S.E. 68, Ga. 1905.

Pierce v. Society of Sisters, 268 U.S. 510, 1925.

Planned Parenthood of Central Missouri v. Danforth, 428 U.S. 52, 1976.

Roe v. Walde, 410 U.S. 113, 1973.

Rowan v. Post Office Department, 397 U.S. 728, 1970.

Sanders v. American Broadcasting Companies, Inc. et al., 20 Cal.4th 907, 85 Cal.Rptr.2d 909, 978 P.2d 67, 15 IER Cases 385, 27 Med. L. Rptr. 2025, 1999.

Shulman v. Group Productions Inc., 74 cal. Rpt. 2d 843, 1998.

Talley v. California, 362 U.S. 60, 1960.

United States v. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 1989.

Watchower Bible & Tract Society of New York v. The Village of Stratton, 122 S. Ct. 2080, 2002.

EU & Member States **Legislation**

Basic Law for the Federal Republic of Germany, (Germany).

Charter of Fundamental Rights of the European Union.

Convention for the Protection of Human Rights and Fundamental Freedoms.

Treaty establishing the European Economic Community (TEEC), Rome, 1957.

LOI n° 78-17 du 6 janvier 1978 - "relative à l'informatique, aux fichiers et aux libertés", (*France*).

Treaty establishing the European Community ("Nice consolidated version").

The Schengen acquis – "Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders".

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

Legge n. 675 del 31 dicembre 1996 - "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", *Garante Per La Protezione Dei Dati Personali*, (*Italy*).

Legge 676/1996, 31 dicembre 1996, (*Italy*).

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".

Data Protection Act 1998, (*United Kingdom*).

D.L. n.135, 11 maggio 1999: "Disposizioni integrative sul trattamento di dati sensibili da parte dei soggetti pubblici", (*Italy*).

Real Decreto 994/1999, de 11 de junio, "por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal", (*Spain*).

D.P.R. n.318, 28 luglio 1999: "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali", (*Italy*).

D.L. n. 281, 30 luglio 1999: "Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica", (*Italy*).

D.L. n.282, 30 luglio 1999: “Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario”, (*Italy*).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (Texto consolidado a fecha 5 de marzo de 2011), (*Spain*).

Provvedimento del Garante per la protezione dei dati personali, n.1/P/2000: “Individuazione dei dati sensibili da parte dei soggetti pubblici", (*Italy*).

Freedom of Information Act 2000, (*United Kingdom*).

Council Directive 2000/78/EC - "Establishing a general framework for equal treatment in employment and occupation", November 27 2000.

The Employment Practices Code (United Kingdom), 2002.

Freedom of Information (Scotland) Act, 2002.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (Directive on privacy and electronic communications).

Informe 327/03 – “Carácter de Dato Personal de La Dirección IP", *Agencia Española de Protección de Datos*, (*Spain*).

Decreto Legislativo 30 giugno 2003, n. 196 - "Codice in Materia Di Protezione Dei Dati Personali", *Garante Per La Protezione Dei Dati Personali*, (*Italy*).

Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre la publicación de sus resoluciones, Agencia Española de Protección de Datos, (*Spain*).

The Environmental Information (Scotland) Regulations, 2004.

LOI n° 2004-801 du 6 août 2004 - "relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

et modifiant la *LOI n° 78-17 du 6 janvier 1978* - "relative à l'informatique, aux fichiers et aux libertés", (*France*).

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".

Real Decreto 1720/2007, de 21 de diciembre, "por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal", (*Spain*).

Consolidated Version of the Treaty on European Union.

Treaty on the Functioning of the European Union (TFEU).

Decreto Legislativo 30 maggio 2008, n. 109 - Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (*Italy*).

Federal Data Protection Act (BDSG) - In the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), (*Germany*).

Directive 2009/136/EC of the European Parliament and of the Council, of November 25 2009, "amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) no. 2006/2004

on cooperation between national authorities responsible for the enforcement of consumer protection laws".

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 com (2012) 11 final 2012/0011 (cod), *European Commission.*

Decreto legislativo 28 maggio 2012, n. 69, Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori. (12G0090)", 2012 (*Italy*).

EU & Member States **Case Law**

Case 26-62 - "NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration". Reference for a preliminary ruling: Tariefcommissie - Netherlands, Judgment of the Court of 5 February 1963.

Case 11-70 – "Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel" - Reference for a preliminary ruling: Verwaltungsgericht Frankfurt am Main - Germany. Judgment of the Court of 17 December 1970.

Case 4-73 – "J. Nold, Kohlen- und Baustoffgroßhandlung v. Commission of the European Communities". Judgment of the Court of 14 May 1974.

Case n. 183 – "Frontini", Italian Constitutional Court, December 27 1973.

Solange I, Beschluß, BVerfGE 37, 271 2 BvL 52/71, 29 May 1974, (*German Constitutional Court*).

Case 106/77 – "Amministrazione delle Finanze dello Stato v Simmenthal SpA". - Reference for a preliminary ruling: Pretura di Susa - Italy. Discarding by the national court of a law contrary to Community law. ECJ, March 9 1978.

Case 44/79 – "Liselotte Hauer v. Land Rheinland-Pfalz". Reference for a preliminary ruling: Verwaltungsgericht Neustadt an der Weinstraße - Germany. Prohibition on new planting of vines. Judgment of the Court of 13 December 1979.

Case 136/79 - "National Panasonic (UK) Limited v. Commission of the European Communities". Competition: Findings of the Commission. Judgment of the Court of 26 June 1980.

Case 294/83 - "Parti écologiste "Les Verts" v. European Parliament". Action for annulment - Information campaign for the elections to the European Parliament. Judgment of the Court of April 23 1986.

Case 170/84 – "Granital", Italian Constitutional Court, June 8 1984.

Solange II-decision, BVerfGE 73, 339 2 BvR 197/83, 22 October 1986, (*German Constitutional Court*).

Maastricht-Urteill, BVerfGE 89, 155, Az: 2 BvR 2134, 2159/92, October 12 1993, (*German Constitutional Court*).

Case C-285/98 - "Tanja Kreil v Bundesrepublik Deutschland". Reference for a preliminary ruling: Verwaltungsgericht Hannover - Germany. Equal treatment for men and women - Limitation of access by women to

military posts in the Bundeswehr. Judgment of the Court of 11 January 2000.

ECJ Opinion 2/00, on *Article 300 (6) TEC*, 2001, § 5.

Joined Cases T-377/00, T-379/00, T-380/00, T-260/01 and T-272/01 - "Philip Morris International, Inc. and Others v. Commission of the European Communities". Decision to bring Legal Proceedings before a court in a non-Member State - Action for annulment - Concept of decision for the purposes of the fourth paragraph of Article 230 EC - Admissibility. Judgment of the Court of First Instance (Second Chamber, extended composition) of 15 January 2003.

Case C-101/01 – "Criminal proceedings against Bodil Lindqvist". Reference for a preliminary ruling: Göta hovrätt - Sweden. Directive 95/46/EC - Scope - Publication of personal data on the internet - Place of publication - Definition of transfer of personal data to third countries - Freedom of expression - Compatibility with Directive 95/46 of greater protection for personal data under the national legislation of a Member State. Judgment of the Court of November 6 2003.

Délibération n° 2006-174 du 28 juin 2006 – "prononçant une sanction pécuniaire à l'encontre du Crédit Lyonnais (LCL) ", *CNIL*, (*France*).

Case C-518/07 - "European Commission v Federal Republic of Germany". Failure of a Member State to fulfill obligations - Directive 95/46/EC - "Protection of individuals with regard to the processing of personal data and the free movement of such data" - Article 28(1) - National supervisory authorities - Independence - Administrative scrutiny of those authorities. Judgment of the Court (Grand Chamber), 9 March 2010.

"The European Commission refers UK to Court over privacy and personal data protection", *European Commission*, *United Kingdom*, Press Room Press releases, 2010.

Joined Cases C-293/12 and C-594/12 - Judgment of The Court (Grand Chamber), 8 April 2014 - "(Electronic communications; Directive 2006/24/EC; Publicly available electronic communications services or public communications networks services; Retention of data generated or processed in connection with the provision of such services; Validity; Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union), Requests for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, received at the Court on 11 June and 19 December 2012, in the proceedings Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others".

Websites

Agencia de Protección de Datos de la Comunidad de Madrid (www.madrid.org), Madrid Community's Privacy Authority.

Agencia Española de Protección de datos (www.agpd.es), Spanish Privacy Authority.

Agencia Vasca de Protección de Datos (AVPD, www.avpd.es), Basque Country's Privacy Authority.

Aljazeera (www.aljazeera.com).

American Civil Liberties Union (www.aclu.org).

Asser Institute (www.asser.nl).

Associated Press (www.bigstory.ap.org).

Association of Defense Communities (www.defensecommunities.org).

Autoritat Catalana de Protecció de Dades (www.apd.cat), Catalan Region's Privacy Authority.

Berliner Beauftragter für Datenschutz und Informationsfreiheit (www.datenschutz-berlin.de), German Commissioner of Berlin.

Blitz Quotidiano (www.blitzquotidiano.it).

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (www.bfdi.bund.de), German Federal Commissioner for Data Protection and Freedom of Information.

Bundesministerium der Justiz und für Verbraucherschutz (www.gesetze-im-internet.de), German Ministry of Justice.

Cornell University Law School, Legal Information Institute (www.law.cornell.edu).

Corte Costituzionale (www.cortecostituzionale.it), Italian Constitutional Court.

Council of Europe (www.conventions.coe.int).

Council of the European Union (www.consilium.europa.eu).

Covington & Burling LLP (www.cov.com).

Daily Mail (www.dailymail.co.uk).

Delegazione di Confindustria presso l'Unione europea (www.confindustria.eu), Italian Industry Association, Delegation to the EU.

Der Spiegel (www.spiegel.de).

El Mundo (www.elmundo.es).

El Pais (www.elpais.com).

Electronic Frontier Foundation (www.eff.org).

Espresso (www.espresso.repubblica.it).

EUR – Lex (www.eur-lex.europa.eu).

Europa Quotidiano (www.europaquotidiano.it).

European Commission (www.ec.europa.eu).

European Court of Justice (curia.europa.eu).

European Parliament (www.europarl.europa.eu).

Find Law (www.findlaw.com).

First Online (www.firstonline.info).

Formiche (www.formiche.net).

Garante Per La Protezione Dei Dati Personali (www.garanteprivacy.it), Italian Privacy Authority.

Governo Italiano (www.governo.it), Italian Government.

Il Messaggero (www.ilmessaggero.it).

Il Secolo XIX (www.ilsecoloxix.it).

La Stampa (www.lastampa.it).

Le Monde (www.lemonde.fr).

Legifrance (www.legifrance.gouv.fr), French government entity responsible for publishing legal texts online.

NPR (www.npr.org).

Polis Blog (www.polisblog.it).

Reuters (www.reuters.com).

Scottish information Commissioner (www.itspublicknowledge.info).

TGCOM24 (www.tgcom24.mediaset.it).

The Guardian (www.theguardian.com).

The Wall Street Journal (www.wsj.com).

The Washington Post (www.washingtonpost.com).

The Wire (www.thewire.com).

UK Companies House (www.companieshouse.gov.uk).

UK Government Legislation Website (www.legislation.gov.uk).

UK Information Commissioner's Office (www.ico.org.uk).

U.S. Department of Homeland Security (www.dhs.gov).

U.S. Department of Justice (www.justice.gov).

U.S. Federal Trade Commission (www.ftc.gov).

U.S. Government Printing Office (www.gpo.gov).

US Legal (www.uslegal.com).

U.S. National Archives (www.archives.gov).

U.S. Senate Committee on Appropriations (www.appropriations.senate.gov).

U.S. Transportation Security Administration (www.tsa.gov).

USA Government, Laws and Regulations (www.usa.gov).

Virtuelles Datenschutzbüro (www.datenschutz.de), German Privacy Authorities.

Wikipedia (www.wikipedia.org).

Wired UK (www.wired.co.uk).

ZDNet (www.zdnet.com).

Thanks to the few who made
this part of my journey happier.
I do not need to mention their names,
for they know who they are,
deep down in their hearts.