ABSTRACT

The object of this thesis is the protection of privacy and personal data in International Law, with a particular focus on the Datagate case and the consequent measures taken by the States and the International Organizations. Furthermore, the second part of the dissertation is focused on the legal framework in Europe and the United States concerning the protection of personal data. The Datagate scandal is essential to understand the urgent need for a new organic combination of international rules, because it gave a concrete perception of the inadequacy and the ineffectiveness of the norms that internationally safeguard these rights. In the first chapter, there is a brief chronology of the case, with particular attention given to the position of the most involved States. The chapter emphasizes the will and the auspice to avoid, in the future, an event such as the mass espionage program established by NSA and other Security Agencies that can strongly affect on people's freedom, as well as the sovereignty of the States. There are several examples of measures taken by the States and some International Organizations in this regard, reflecting the fact that there are many pressures to give a different, richer and more comprehensive regulation to a matter that International Law still does not fully face. For example, the data protection Supervisors of the world, during the 35th conference held in Warsaw in September 2013, adopted a resolution on the subject of digital education in which governments are encouraged to promote a common educational program for their citizens. The European Union has taken a large amount of measures at different levels, giving rise to combined efforts coming from the Commission, the Parliament and the Court of Justice. The former proposed a structural reform of the European legal framework for the protection of personal data. The second proposed a joint resolution against the PRISM espionage program. The latter issued a landmark ruling on the fundamental *right to be forgotten*. Even in the United States, the undeniable protagonist of the Datagate scandal, there have been important changes after the explosion of the case, so much so President Obama has called for the drafting of a text drafted by experienced technicians. They require important steps for the protection of non-American citizens, as well as concrete measures to promote transparency and accountability, so that any violations could be properly punished. The American experts emphasize, in the text, the importance of the courts in order to give permissions to proceed, openly opposing

any form of data mining for intelligence purposes. The most important initiatives have been taking within the General Assembly of the United Nations, where an important discussion on numerous issues on the case is still taking place. A proposal for a real code of ethics against unscrupulous, unregulated espionage, reaffirming the right to privacy, has been proposed by Germany and Brazil, having a strong favour within the GA. This proposal became the resolution 68/167, which strongly emphasizes the negative impact of mass surveillance and extraterritorial wiretapping on the enjoyment and exercise of human rights. In the text, there is a very important principle, often invoked by the Authorities for the protection of privacy around the world: the same rights that people have offline must also be maintained, protected and respected online. The resolution recognizes, therefore, that respect for the right to freedom of expression and at the same time the protection of online privacy are the key to create confidence in the internet users; it also states that any attempt by an individual to deal with security problems on the Internet must therefore be consistent with international human rights obligations. The resolution states, indeed, that everything must be ensured through transparent and democratic institutions, based on the rule of law. States are finally called, according to the Fourth operational proposition, to respect Human Rights in the context of digital communications; they shall protect people against interception, collection and reprocessing of indiscriminate data, and more generally against mass surveillance in communications.

The second part of the dissertation focuses on the comparison between the European and the American legal system in the matter of protection of privacy and personal data. This comparison is fundamental because it stresses the role of European Union in the Datagate case: indeed, even if the PRISM program comes from the United States, it spreads around the world, having Europe as one of its main subject of data mining. The interesting aspect is that the Old Continent has a large amount of juridical safeguards against the unqualified appropriation of personal data, so the Datagate case emphasizes the ineffectiveness of these rules. The second part of the thesis has the aim to identify the structural differences between the two systems, with the ultimate goal to find a compatibility between the American monitoring plan and the regulatory systems in Europe and the United States in this matter. In the field of protection of personal data, there are substantial differences between the two sides of the Atlantic Ocean. While in the European case the right to privacy and the right to

protection of personal data are elevated to the status of fundamental rights, in protection of which there is a well-defined regulatory structure, we cannot say the same for the American case. The above-mentioned rights in fact, in the context of the American legal system, can be easily disregarded in favour of a series of anti-terrorism measures. In other words, borrowing a terminology closer to the philosophy of law, in the trade-off between freedom and security in the area of privacy and data protection, Europeans are normatively more careful of freedom than the Americans. In the European case, in fact, article 8 of the ECHR covers a broad range of interests related to the right to privacy and the protection of personal data. It sets out exceptions to the right to privacy only when the interference is unavoidable and such "intrusions" are implemented in the name of a legitimate aim (eg. Public safety), respecting the principle of necessity ad proportionality. Moreover, even the European Union provides for specific rules on the matter in question. In this case, the Convention n. 108 and Directive n. 95/46 / EC require a number of additional parameters on the rules governing the protection of personal information. Among them, in Directive 95/46, the most significant are undoubtedly the principle of *data quality* and the *enhanced protection of sensitive data*. Regarding the transfer of data to non-EU Countries, Article 25 of Directive 95/46 stipulates that it must only be carried out if those Countries ensure an adequate level of protection. As is known, the United States do not provide the same protection systems put in place in the European Union: the permissions to store sensitive personal informations, already widely granted by United States law, have increased because of the terrorist attacks of 2001 and the consequent USA Patriot Act. Therefore, the last part of the second chapter tries to explain how the mass transfer of a huge amount of data and metadata from Europe to the United States authorities has been made possible. This part focuses on a sort of "normative bridge" that links the European and the US legal system in the field of data protection. Indeed, the so-called Safe Harbor is the result of formal agreements between the two sides of the Atlantic Ocean, which allows bypassing the restrictions regulated in Article 25 of Directive 95/46 / EC on the transfer of European data to non-European countries, having regard of a future trade agreement between the transatlantic Allies. This system is based on the voluntary acceptance, by US companies operating in Europe, to a set of principles. The enterprises must notify the adherence to the Safe Harbor at the Department of Commerce, which compiles an annual list of the member companies. Once the notification has been sent, such companies have a legal obligation to respect the principles mentioned above,

which are nothing other than the main European standards of data protection and privacy. Given that there has actually been adherence to the Safe Harbor mechanism by all telecommunications companies involved in the scandal Datagate, there is an existent incompatibility between European standards and the PRISM program. In conclusion, if on the one hand the United States does not have a particular mechanism of protection from abuse of data mining, on the other hand Europe is not able to apply effectively the safeguards that its own legal system already includes. Therefore, Europe should use a number of devices to ensure the observance of the fundamental rights to privacy and protection of personal data. In addition, in a globalized system that has its main archive of informations on the Internet, even the United States should organize its regulation on this field in an organic system, developing a different approach on the principles that compose the common legal substratum on the rights to privacy and protection of personal data.

The last part of the dissertation deals with the most significant drawbacks highlighted by the Datagate scandal in a more general way: in this conclusive section stresses the potential negative impact that the so-called *digital Tsunami* of the social networks can have on public relations as well as individual rights. It is therefore implied the need for a new approach of international law to the delicate matter of the protection of privacy and personal data in cyberspace. Therefore, the right of access to the Internet should be regulated by specific rules, taking into account a number of international agreements in the field of data protection. The concept of common regulation also connects another peculiar feature of the web. The latter, in fact, has no boundaries. For this reason, in the rare cases in which States have managed to limit accesses to the Internet, this was followed out with great difficulty and at the cost of immense restrictions of the freedom of the press and of association. It is consequently not desirable to preclude accesses – infringing article 19 of the UDHR on the right to seek and receive information-, but to regulate conscious accesses. In this section is finally listed a series of measures, also suggested by leading jurists, that can give thrust to a concrete modification of International Law in order to have a more organic and all-encompassing legislation in an area which, by the very nature of the Internet, may not be the addressed except through a concerted international effort. First of all, the responsible handling of sensitive data, in compliance with the principles of proportionality and purpose limitation, as well as the fundamental right to be forgotten. In addition the States (US above

all) should thin the discrepancy that exists between the national data processing and data processing of foreign Countries. From here on, a more general reflection on the privacy and fundamental freedoms in the digital age takes hold: the human being, which in our time has given birth to a digital creature inextricably linked to the individual's identity, now requires an effective defence of its "electronic body". From here starts the development of the concept of *Habeas Data*, borrowed from the much more famous *Habeas Corpus*, thanks to which the first steps in the history of the development of personal freedoms began to be covered. The relevance of this issue is very clear, in that it addresses the issue of mass surveillance and the arbitrary appropriation of sensitive data that toady are presented as a considerable part of the identity of a human being. International Law should play an active role in this matter, trying to impose general binding rules on all Member States. Without a minimum cooperation in the international arena, the ineffectiveness of this initiative is almost assured. The actions in the General Assembly of the United Nations, in particular the recent resolution that has as its major promoters Germany and Brazil, are indicative of a clear desire to move in this direction, but it still does not seem enough. The right to privacy and protection of personal data in the digital age is reasonably complicated to discipline, but it should become part of that mandatory law belonging to each individual. If these alternatives were taken into account, the threat of a new Datagate would be averted, privacy and freedoms related to it would be effectively respected, and the Internet would be no more than an invaluable resource to which there is no need to feel vulnerable.