Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

JACQUELINE HELLMAN*

NATIONAL SECURITY AND CITIZEN'S RIGHTS: WALKING TOWARDS A DYSTOPIAN ORWELLIAN STATE?

SUMMARY: 1. Surveillance programs implemented by European countries. - 2. Citizens' rights at risk when implementing surveillance programs? - 3. Compatibility with the supranational European legal order? - 4. Conclusions.

1. *Surveillance programs implemented by European countries*

Large scale of surveillances practices has been carried out in the last decades by many different governments. A few years ago, in 2007, the US National Security Agency (NSA) launched a relevant program, called PRISM [1], focused in targeting encrypted communications and, therefore, enabling the access to personal information of millions of Internet users. This kind of strategy enhanced by powerful states, has given rise to ethical and legal questions: is the gathering of information valid when done exclusively for the sake of protecting national security interests? Even if it is so, should this data harvesting be subjected to certain limits as the fulfilment of the basic and fundamental rights of individuals? Moreover, are the actual government's programmes for mass surveillance respecting the supranational legal order?

All these thorny questions – which will be discussed in detail later on – are strongly linked to the reasons and justifications frequently brought out when arguing in favour of the existence, legitimacy and continuity of the above-mentioned surveillance programs. In this sense, it is important to highlight, that the US government has strongly sustained that the powerful mechanisms of surveillance are not used for domestic targets if no warrant orders have been rendered; supporters of this type of technology claim that it prevents, among others, the perpetration of terrorism acts. In fact, US President Obama, when visiting – in 2013 – German Chancellor Angela Merkel in Berlin, commented that this data

* Senior Lecturer at Universidad Europea de Madrid.

[1] This program, launched by former President George W. Bush, appeared with the Protect America Act of 2007. One year after, FISA Amendments Act was adopted stating that companies were exempted from being subjected to legal actions when collecting intelligence information in cooperation with the US government.

gathering carried out by specialized bodies is a positive strategy as it is helping *de facto* to save lives[2]. On another occasion, Obama putting the finger on the wound maintained the following idea: «You can't have 100 per cent security and also have 100 per cent privacy and zero inconvenience (…). We're going to have to make some choices as a society. On balance we have established a process and a procedure that the American people should be comfortable about[3]». From the words of the current US President, there is no doubt that the implementation of surveillance programmes constitutes a sensitive issue, as the compilation of information cannot be reduced to a discussion between those strategies and the protection of national interests. It goes beyond that: this analysis has to be necessarily done on the basis of legality and respect of basic rights.

Either way, it is important to stress that this telecommunication infrastructure of mass oversight has not only appeared in the US. The European Union (EU) countries are also playing an important role in this not so new phenomenon. In the UK, surveillance operations have taken place through the Government Communications Headquarters (GCHQ), being by far the most engaged member state in collecting systematic personal information and, inevitably, the one that has caused the biggest impact on the rights of European citizens. Indeed, the responsibilities assumed by the British intelligence agency are mainly to ensure the protection of national security, to prevent and detect serious crimes and to give support to military operations all across the world[4]. However, on many occasions, the GCHQ has gained significant and indiscriminate information of the web and mobile phone networks, undermining the privacy of individuals[5].

Other countries, such as France, are also implementing similar electronic surveillance activities. We cannot compare it with the abovementioned states in terms of budget and capacity but although, to a lesser extent, the French national strategies established to obtain personal information is having a wide-reaching repercussion on the sphere of citizens' rights[6]. As an example, we have to take into account a recent law adopted in December 2013[7] – that will not take effect until next year – that has empowered French agencies, government, public officials including police to spy on internet users by monitoring computers, tablets and smartphones, without the necessity of asking for authorization[8]. Article 20 of the referred regulation, known as *Loi de Programmation Militaire*[9], has broadened the French surveillance power by stating that the competent bodies – security forces and intelligences services – will be able to check the content of electronic and digital

---

[2] Information hereby provided (accessed November, 2014): http://www.cbsnews.com/news/obama-defends-narrow-surveillance-programs/

[3] Information hereby provided (accessed November, 2014): http://swampland.time.com/2013/06/07/president-obama-defends-nsa-surveillance-programs-as-right-balance/.

[4] *Vid.* G. O' DONNELL, *Government Communications Headquarters (GCHQ): Baseline Assessment* in *Capability Reviews. Civil Service*, 2009.

[5] Information hereby provided (accessed November, 2014): http://www.theguardian.com/law/2013/oct/13/gchq-surveillance-right-challenge-state-law; http://www.bbc.com/news/world-us-canada-23123964

[6] *Vid.* D. BIGO, S. CARRERA, N. HERNANZ, J. JEANDESBOZ *et. al.*, *National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU Law* in *Directorate General for Internal Policies. Policy Department C: Citizens' Rights and Constitutional Affairs,* 2013.

[7] Information hereby provided (accessed November, 2014): http://www.lemonde.fr/international/article/2013/12/10/adoption-definitive-de-la-controverse-loi-de-programmation-militaire_3528927_3210.html

[8] This regulation was adopted a few days after the protests led by President Francoise Hollande took place regarding the oversight activities carried out by the NSA that affected many European citizens, including French nationals.

[9] Information hereby provided in (accessed November, 2014): http://www.senat.fr/leg/tas13-046.html

communications in real time, to discover who is connected to whom and where they are located. This has been done on the grounds of safeguarding national security; preventing terrorism and organised criminality; protecting essential national economic and scientific interests and acting against hate groups.

Sweden, an increasingly important actor in terms of collecting data information, has also carried out oversight operations – mainly by monitoring Internet telecommunications – through *Försvarets radioanstalt* (RFA), which has strongly cooperated with some of its counterpart's abovementioned and, therefore, has been severely criticized for dealing with significant personal data[10]. Despite the popular concern that commonly appears when discussing these matters, the Nordic country passed, in 2008, a law enabling the referred intelligence agency to develop mass surveillance programs in order to obtain information regarding cross border emails, as well as phone communications without the need of obtaining judicial authorizations, aligning supposedly the content of these programs with the protection of Swedish interests[11].

Germany and Spain also have intelligence agencies with significant surveillance power working in cooperation with their counterparts. In fact, according to the British intelligence agency, the *Bundesnachrichtendienst* (BND) – the Germany's federal intelligence service – has «huge technological potential and good access to the heart of the Internet[12]», and has been assisted to change and circumvent its own regulation in order to facilitate spy activities[13], as Germany has a strong legal framework regarding the protection of privacy. Very similarly, the Spanish intelligence agency, *Centro Nacional de Inteligencia* (CNI) – according to an official and secret document entitled "Sharing computer network operations cryptologic information with foreign partners" –, has collaborated with NSA in terms of storing personal data[14], revealing that the Spanish government has openly failed to protect the rights and privacy of its citizens, despite the fact that *Centro Criptológico Nacional* (CCN) should have ensured the protection of classified information as it was created *ex professo* for that reason[15].

As a consequence of the above situation in which tight relationships between intelligence agencies have appeared[16] and the approval of new regulation facilitating the gathering of personal information constitutes a reality in many different countries, we can hold that one of the most important priorities of many European governments is to put

[10] Information hereby provided (accessed November, 2014): http://www.thelocal.se/20131103/bildt-defends-sweden-surveillance

[11] In 2008, a regulation passed in Sweden, named Government Bill 2006/07:63 Adapted Defence Intelligence Operations, encouraged the right to gather and analyse all communication data -including Internet traffic, electronic mails, text messages, faxes, and telephone conversations- that could be regarded as a threat to the interests of the Swedish Kingdom. Information hereby provided (accessed November, 2014): http://www.regeringen.se/sb/d/8670/a/78367

[12] Information hereby provided (accessed November, 2014): http://www.reuters.com/article/2013/11/02/us-europe-surveillance-idUSBRE9A103K20131102.

[13] *Ibidem.*

[14] Information hereby provided (accessed November, 2014): http://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html

[15] Information hereby provided (accessed November, 2014): https://www.ccn.cni.es

[16] However, it seems that this close relationship between intelligence agencies is not an obstacle for the perpetration of acts of espionage between them. According to recent information provided by a former agent of NSA, Edward Snowden, we have to highlight the spying activities carried out by the US intelligence agency in German territory. Information hereby provided (accessed November, 2014): http://online.wsj.com/articles/u-s-spying-on-germany-unacceptable-says-merkel-1405174452

the needs for the protection of national interests and the avoidance of terrorist attacks before any other consideration.

Taking this into account, it is easy to understand why today the EU is anything but reluctant to establish a supra national policy in charge of coordinating the security and surveillance activities of all member states. In this sense, it should be noted that the relevant strategy implemented – since 2002 – by the European Unions' Joint Situation Centre (SitCen), a body in charge of such coordination through the sharing of vital information. However, according to Davis Cross, SitCen «(…) has no formal mandate to engage in intelligence gathering, traditionally understood, and relies to some extent on intelligence provided by member states on a voluntary basis[17]». In any event, this is not the only initiative forged by the EU. A few years later, in 2005, the European Commission presented a legal proposal regarding data retention when fighting against terrorism, establishing temporal storage of telephone calls and Internet traffic. At that time, the Commissioner for Justice and Home Affairs, Franco Frattini, said that Europe should not encourage safe havens for terrorists and, from his point of view, having more than twenty legal different regimes – concerning the matter here discussed – helps them to receive "shelter"[18]. Thus, one year later, Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks entered into force[19]. This European legal instrument, in its preamble, showed its concern towards the protection of the rights and freedoms of European citizens with regard to the processing of personal data. This legal tool dealt with preventing, investigating and detecting criminal offences and, at the same time, tried to ensure that the gathering of personal information was done exclusively for such purposes. However, a recent sentence rendered by the Court of Justice of the EU (CJEU) states that the above-mentioned Directive is not compatible with the Union's Charter of Fundamental Rights and not valid as it «entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data[20]».

Likewise, in this field, we have to recognize the crucial role-played by the European Union Police Office (Europol), which in charge of dealing with criminal information, promotes and eases the exchange of vital information between member states. In terms of

---

[17] *Cfr.* K. M. DAVIS CROSS, *EU Intelligence Sharing & The Joint Situation Centre: A Glass Half-Full*, document prepared for delivery at the 2011 Meeting of the European Union Studies Association March 3-5, 2011.

[18] Information hereby provided (accessed November, 2014): http://euobserver.com/justice/19909
Other similar measures recently adopted, such as Regulation 1052/2013, evidenced the need of stimulating coordination between national bodies in order to facilitate the exchange of vital information that may pose a threat to European territory. For this reason, the referred legal tool states the following: «the establishment of a European Border Surveillance System ('EUROSUR') is necessary in order to strengthen the exchange of information and the operational cooperation between national authorities of Member States as well as with the European Agency for the Management of Operational Cooperation at the External Borders of the Member States (…) for the purpose of detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants». Information hereby provided (accessed November, 2014): http://frontex.europa.eu/assets/Legal_basis/Eurosur_Regulation_2013.pdf

[19] Information hereby provided (accessed November, 2014): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[20] It refers to the judgment rendered on 8th of April of 2014 by the CJEU regarding *Cases C-293/12* and *C-594/12*, in InfoCuria. Information hereby provided (accessed November, 2014): http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

mass surveillance, a Joint Supervisory Body (JSB) has been created in order to ensure that European countries are fully complying with the main data protection principles. As the Economic Crime Division of the Council of Europe has stated, the JSB «reviews all activities of Europol in order to ensure that the rights of the individual are not violated through the storage, processing and utilisation of their data held by Europol. It also monitors the permissibility of the transmission of data originating from Europol[21]».

Thus, we have seen important efforts made by some European institutions when trying to ensure legal and common procedures when collecting data for the purpose of investigating and detecting the perpetration of serious crimes. However, European member states have deliberately and jealously kept their competence over data protection in order to avoid the interference of EU institutions. In consequence of this, European countries are still able to decide about the content of surveillance programs with almost unlimited room for manoeuvre. Therefore, the EU cannot promote a meaningful development, as this international organization has little power over this controversial and complex subject[22].

2. *Citizens' rights at risk when implementing surveillance programs?*

Surveillance measures, seen sometimes as "Orwellian strategies", have been implemented in these last years due to the fact that governments want to tackle terrorism, organised crime, and illegal immigration. Nevertheless, government policies are at the centre of an on-going debate as many scandals have appeared recently, highlighting the disputed practices applied by the previously mentioned intelligence agencies. After all this uproar, many people think that the separation between surveillance made for criminal reasons and an indiscriminate one not subjected to limitations is nowadays getting blurrier[23].

In this sense, we have to mention once again the disclosure of NSA files made last year by Edward Snowden[24]. Through declassified documents provided to some journalists

---

[21] *Cfr.* R. VAN DEN HOVEN VAN GENDEREN, *Cybercrime investigation and the protection of personal data and privacy* in *Economic Crime Division. Directorate General of Human Rights and Legal Affairs. Council of Europe,* 2008.

[22] *Ibidem.* «Still, criminal procedures, surveillance, investigation and enforcement procedures are considered national competence areas. (…) nations are still reluctant to hand over responsibility for law enforcement to a supranational level».

[23] In this sense it must be highlighted that «the distinction between targeted surveillance for criminal investigation purposes, which can be legitimate if framed according to the rule of law, and large-scale surveillance with unclear objectives is increasingly blurred». *Cfr.* D. BIGO, S. CARRERA, N. HERNANZ, J. JEANDESBOZ *et. al.*, *National programmes…,* cit.

[24] Edward Snowden -the computer analyst whistle blower- provided, among other things, information about the secret files of the NSA, which revealed the US controversial surveillance strategies used on telephone calls and Internet communications. Information hereby provided (accessed November, 2014): http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?_r=0. He also disclosed the oversight programs implemented by other intelligence agencies, such as *Tempora*, a British surveillance tool designed for storing data information from fibre-optic cables for up to thirty days. According to "The Guardian" – the newspaper that has provided all this controversial information –, *Tempora* «represents a window on to their everyday lives, sucking up every form of communication from the fibre-optic cables that ring the world». Information hereby provided (accessed November, 2014): http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

he called into question the controversial actions carried out by the US intelligence agency, which conducted mass surveillance practices that collided with the rights held by many individuals all around the globe. Information about similar strategies followed by other agencies has been also reported to the international press. This is the case of the GCHQ that presumably undertook large-scale surveillance of digital communications, obtaining data secretly from the most important Internet companies[25]. In the same vein, the German intelligence agency sent significant amount of information to NSA[26], just as the Swedish one, which shared access to communication cables in the Baltic Sea based on the idea of avoiding the application of domestic regulation[27].

All these revelations stemmed from the deliberate leaks yield by Snowden are evidencing many of the pitfalls detected when applying this technology. Consequently, it is vital to consider if, in strict compliance with the relevant legislation, basic principles and rights are respected when collecting data information. Without doubt, some protection standards need to be fulfilled when fighting against terrorism. Not everything is acceptable for the sake of national protection. In this respect, as the Commissioner for Human Rights established by the Council of Europe, Nils Muižniek, said: «the fear of terrorism, technology that is developing at the speed of light, private companies and state security agencies compiling personal information – this topical mix has become a severe threat to the right to privacy. Despite the intentions, secret surveillance to counter terrorism can destroy democracy, rather than defend it[28]».

Accordingly, it is easy to understand why these data-gathering methods are under scrutiny and why it can be argued, on many occasions, that the intelligence activities encouraged by some governments are enhancing the displacement of democratic regimes to police states. When this indiscriminate and irresponsible use of mass surveillance practices take place – in which it seems that we are all carrying our own "pocket sensors" – a question that summarises quite much the subject arises: are we walking towards a "*dystopian Orwellian state"* when applying measures that affect our very essence of the right to privacy? To solve this enigma, it is crucial to analyse the referred national surveillance programmes under the legal framework of fundamental rights and freedoms in order to determine if the above-mentioned practices successfully overcome or not a "*dystopian state test"*.

3. *Compatibility with the supranational European legal order?*

Data protection is a basic right that needs to be protected – particularly in this digital world in which we live – and, of course, at the same time we also recognize the importance

[25] Information hereby provided (accessed November, 2014): http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

[26] Information hereby provided (accessed November, 2014): http://www.spiegel.de/international/world/spiegel-reveals-cooperation-between-nsa-and-german-bnd-a-909954.html

[27] Information hereby provided (accessed November, 2014): http://www.thelocal.se/20131211/sweden-aided-in-nsa-hacking-operations-report; http://www.wikileaks-forum.com/impact-of-the-leaks/334/sweden-a-close-partner-in-nsa-surveillance/22686/

[28] Information hereby provided (accessed November, 2014): http://humanrightscomment.org/2013/10/24/human-rights-at-risk-when-secret-surveillance-spreads/

of preventing and detecting serious crimes. The question is if we can reconcile these two needs. This concern, which has no easy solution, has been addressed in the following way: «There must be an open eye for threats to society, internal and external, but fundamental rights such as privacy must be considered of great value for a democratic society and must be available for all persons on an equal basis[29]». How should we establish the relationship between security and privacy? Can we really find equilibrium between these two ideas? When analysing the surveillance practices carried out by some states in the precedent years, it seems that there is no possible balance between the former, as the evidence shows us that the weight has fallen entirely in favour of the protection of national security interests[30]. Moreover, after reading the declassified materials provided by Edward Snowden one could easily think that powerful countries with strong technology are able to enhance widespread privations of rights and freedoms with almost no constraint. Likewise, on the same lines, recent regulations adopted, such as the "Retention Directive" of 2006, demonstrate that the communication service providers can retain vast data information, giving up consequently on the protection of privacy rights.

Notwithstanding the foregoing, which provides a poor picture from the perspective of basic rights regulation fulfilment, it is important to stress the existence of significant supranational legal provisions encouraging policy privacy rights. In this sense, it is vital to highlight that the international community has to follow and duly apply article 17 of the International Covenant on Civil and Political Rights[31] and, in particular, European states, according to article 8 of the European Convention on Human Rights, should respect private and family life[32]. In this respect, the European Court of Human Rights sustained, the 27th of August of 1997, regarding the case of M.S. v. Sweden the following idea: "Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention". The sentence rendered in this case clearly stated that disclosure of private information could only take place when proportionate to the legitimate aim pursued. This, *grosso modo*, coincides with the judgement rendered by the referred court the 4th of December of 2008 in the case S. and Marper v. UK.

Quite similar is article 7 of the European Union's Charter of Fundamental Rights: «Everyone has the right to respect for his or her private and family life, home and communications[33]». As the Council of the EU has declared, the above-mentioned legal provision encompasses developments in technology, as the word "correspondence" has been substituted by "communications", anticipating the existence of the type of conflicts hereby discussed. Article 8 of the latter document is also relevant in so far as it refers to the

---

[29] *Cfr.* R. VAN DEN HOVEN VAN GENDEREN, *Cybercrime investigation,* cit.

[30] «In the international treaties on human rights, data protection and/or the protection of privacy and/or personal life are widely considered to be building stones of a civilized society, although in 90% of the world the recognition of this principle is no guarantee that it is actually followed in national practice» (*Ibidem*).

[31] Article 17 reads as follows: «1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks».

[32] Article 8 states the following: «1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others».

[33] Information hereby provided (accessed November, 2014): http://www.europarl.europa.eu/charter/pdf/text_en.pdf

protection of personal data. Consequently, regarding the supra national regulation in force, «(…) European states are obliged to protect individuals from unlawful surveillance carried out by any other state and should not actively support, participate or collude in such surveillance[34]».

In this context, basic guidelines have been adopted by relevant international organizations, such as the Organisation for Economic Co-operation and Development (OECD), outlining general principles that should be regarded as minimum national standards when protecting privacy and individual liberties[35]. These guidelines mainly refer to the limits that should be imposed when collecting personal data, pointing out the need that it has to be obtained lawfully and by fair means, it has to be relevant to the purposes for which they are going to be used, etc. Yet, the United Nations (UN) adopted, on December 1990, a few relevant guidelines concerning computerized personal data files[36]. According to the UN, governments should include in their domestic regulations the principle of lawfulness and fairness, the principle of accuracy, the principle of the purpose-specification, the principle of non-discrimination, etc., in order to duly protect essential rights.

The most positive thing is that there is not only significant regulation giving priority to the protection of basic privacy rights, but also relevant jurisprudence pointing out in this same direction[37]. As we previously saw, the CJEU has ruled that the discussed Directive of 2006 is not compatible with the Union's Charter of Fundamental Rights. The sentence specifically says that the data «(…) retained [through the mechanisms provided in such legal tool] and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance[38]». Following on from that, the court makes an important statement: «(…) as regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against

---

[34] *Vid. Supra*, Footnote 28.

[35] Information hereby provided (accessed November, 2014): http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[36] Information hereby provided (accessed November, 2014): http://www.refworld.org/pdfid/3ddcafaac.pdf

[37] In the US, relevant rulings have been issued regarding the implementation of disputed oversight programs. In this sense, we have to highlight the statement made by the US District Court Judge, Richard Leon, who said that the NSA programs in charge of obtaining information from telephone calls are «likely unconstitutional». Information hereby provided (accessed November, 2014): http://www.politico.com/story/2013/12/national-security-agency-phones-judge-101203.html. Also, North American judges when analysing the activities carried out by the NSA, have invoked the US Fourth Amendment that refers to the prohibition of executing unreasonable search and seizure. All this has resulted in what is now known as the "magistrates revolt" in which a significant number of sentences have been rendered denying the government request of obtaining unlimited and broad search warrants. Information hereby provided (accessed November, 2014): http://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html Likely, domestic judicial systems of other European countries are working hard in the protection of privacy rights. For instance, German prosecutors are investigating the alleged espionage done by the NSA to Chancellor Angela Merkel's cell phone. Information hereby provided (accessed November, 2014): http://www.huffingtonpost.com/2014/06/04/nsa-merkel-phone-tap_n_5444440.html.

[38] *Vid. Supra*, Footnote 20. This case refers to a court action brought by Digital Rights Ireland Ltd. against Ireland regarding domestic data-retention regulation in which it was established that telephone companies and internet service providers had to obtain information about the location of customers and store it for up to two years.

organized crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight». Accordingly, the European regulation did not ensure the safeguards stipulated in article 8 of the Charter. Clearly, untargeted monitoring is not acceptable in European democratic societies[39].

We have to underline once again the significant impact that the above-mentioned sentence rendered the 8th of April of 2014 -by the CJEU- has. According to Boehm and Cole, the CJEU concludes that "(...) the retention of data for the purpose of possible later access by the competent national authorities directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 CFR[40]". Without doubt, the above-mentioned ruling does not entrench the European regulation in the area of protection and security. In fact, privacy rights are now better protected than before, as it has been agreed that restrictions to escort national security can only be legally imposed when they are necessary, appropriate and proportionate[41]. Therefore, mass surveillance practices within a democratic society cannot take place if they do not entail the full accomplishment of certain basic guidelines and principles, already designed by some international organizations[42]. Thus, *a test of necessity, appropriateness and proportionality* has to be done when analysing measures of data gathering in order to duly determine if those may or may not imply the potential establishment of a "*dystopian state*"[43].

In view of this, surveillance programmes exceeding the limits imposed by the principles referred or not exercising them in a manner that are adequate, relevant and not excessive in relation to the purpose of the interference are not acceptable under any circumstance. As explained, Boehm and Cole, among others, support a similar idea after analysing the sentence previously mentioned[44], which unquestionably plays an important role. Indeed, the ruling rendered the 8th of April of 2014 clarifies quite much the issue analysed in this paper, in the same way as many others do when highlighting the utility of

---

[39] In this respect, Boehm and Cole argue that: "The Court confirms that the retention of data for the purpose of possible later access by the competent national authorities directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 CFR". *Cfr.* F. BOEHM, M. D. COLE, *Data Retention after the Judgement of the Court of Justice of the European Union*, 2014, p. 28. Document hereby provided (accessed November, 2014): http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

[40] *Ibidem.*

[41] Information hereby provided (accessed November, 2014): http://www.theguardian.com/commentisfree/2014/jun/05/what-snowden-revealed-changed-nsa-reform

[42] The European Court of Human Rights has fast-tracked a case about the activities carried out by GCHQ. The Court tries to establish if the British intelligence agency has complied or not with article 8 of the European Convention on Human Rights. Information hereby provided (accessed November, 2014): http://www.theguardian.com/uk-news/2014/jan/24/justify-gchq-mass-surveillance-european-court-human-rights

[43] The European Parliament, in its resolution of 4 July 2013, calls on the Commission to ensure European standards on data protection, demanding member states to check if their surveillance programs are compatible with the European regulation, including the fundamental rights established in the European Charter. Information hereby provided (accessed November, 2014): http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN&language=EN

[44] *Cfr.* F. BOEHM, M. D. COLE, *Data Retention after the Judgement of the,* cit., p. 32 and following.

balancing the protection of privacy rights when retaining data for investigation and prosecution of crimes against the interest of states[45]. Analysing the outcome of the cases that have been previously mentioned leads us to argue that when collecting personal information the protection of privacy rights is vital to a person's enjoyment of his or her right to respect for private life. There is no doubt that "any infringement of fundamental freedoms under EU law must satisfy the fundamental rights test in order to survive scrutiny[46]".

4. *Conclusions*

The documents leaked, last summer, by former NSA analyst Edward Snowden to the international press revealed that programs, such as PRISM, enabled governments to access and process, all around the world, large-scale personal data. As we have seen, the referred US intelligence agency used intrusive techniques of surveillance, including the interception of communications worldwide. Unfortunately, European counterparts have carried out similar practices that implied the information retrieval of millions of devices, despite the fact that they are obliged to respect fundamental rights and values enshrined, among others, in the Charter of Fundamental Rights. However, as it could not have been otherwise, today some of these strategies are on suspect, such as the ones carried out by the British intelligence agency, which has been accused of breaching the right to private and family life regarding article 8 of the European Convention on Human Rights.

Of course, as it was said before, we do stress the importance of fighting against the perpetration of heinous crimes but, at the same time, it is crucial when data gathering takes place to protect basic rights and freedoms. In other words, the end does not justify the means. Accordingly, strong internal controls must be imposed in order to safeguard and put in place the highest ethical standards so as to guarantee democratic sates based on the rule of law, just as the European Parliament has recently noted[47]. On the contrary, giving countries and their intelligence agencies arbitrary powers through unrestrained de-regulation, not monitoring surveillance systems, etc., would lead to the establishment of policy states. Therefore, there is a need to establish a test of necessity, appropriateness and proportionality as from the moment data harvesting is used as a technique for the collation of personal information. This test would enable us to determine if concrete mass oversight practices are or are not heading towards the establishment of a "*dystopian Orwellian state*", where totalitarian and indiscriminate measures are imposed.

Be that as it may, it is clear that the documents provided by Edward Snowden have not only triggered a huge outcry, but also positive outcomes. Since those revelations were made, companies have focused in the protection of privacy rights by changing their policies

---

[45] Sentence rendered by the European Court of Human Rights the 18th of April of 2013 regarding M.K. v. France case.

[46] *Cfr.* F. BOEHM, M. D. COLE, *Data Retention after the Judgement of the,* cit., p. 45.

[47] «(…) citizens have a right to know about serious violations of their fundamental rights and to denounce them, including those involving their own government; stresses the need for procedures allowing whistle-blowers to unveil serious violations of fundamental rights and the need to provide such people with the necessary protection, including at international level; expresses its continued support for investigative journalism and media freedom». *Vid. Supra.* Footnote 43.

in case of surveillance requests and, also, asking governments for more transparency when cooperating with intelligence agencies[48]. In addition, European supranational courts, European domestic tribunals and US judges are now examining questionable large-scale surveillance practices. Moreover, supranational institutions, such as the European Commission, are enhancing new and updated data protection standards[49]. Likewise, the UN has launched an investigation regarding the dubious actions carried out by the US and by British intelligence agencies[50]. All of the above, is quite probably the consequence of a significant increase of public awareness to foster respect towards basic rights, which is very much in line with Snowden's words: «I didn't want to change society. I wanted to give society a chance to determine if it should change itself[51]». Therefore, with the information now in our hands, we have to decide if we either give support to states in which intelligence agencies are behind the shadows preventing serious crimes but also leaving no room for our privacy rights or encourage reasonable and proportional governmental measures when trying to avoid the perpetration of such illicit. It seems that now the scales are tipping towards the latter point of view. However, we must remain vigilant. Reality will give the game away...

BIBLIOGRAPHY

D. BIGO, S. CARRERA, N. HERNANZ, J. JEANDESBOZ *et. al.*, *National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU Law* in *Directorate General for Internal Policies. Policy Department C: Citizens' Rights and Constitutional Affairs,* 2013.

F. BOEHM, M. D. COLE, *Data Retention after the Judgement of the Court of Justice of the European Union*, 2014

J. CRAWFORD, *Brownlie's Principles of Public International Law*, Oxford University Press, 8th Edition, 2013.

K. M. DAVIS CROSS, *EU Intelligence Sharing & The Joint Situation Centre: A Glass Half-Full*, document prepared for delivery at the 2011 Meeting of the European Union Studies Association March 3-5, 2011.

G. DI FEDERICO, *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument Ius Gentium: Comparative Perspectives on Law and Justice*, Springer, 2010.

[48] Information hereby provided (accessed November, 2014): http://mashable.com/2013/09/09/google-petitions-transparency/; http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html

[49] Information hereby provided (accessed November, 2014): http://www.theguardian.com/world/2013/oct/17/eu-rules-data-us-edward-snowden.

[50] Information hereby provided (accessed November, 2014): http://www.theguardian.com/world/2013/dec/02/edward-snowden-un-investigation-surveillance

[51] Information hereby provided (accessed November, 2014): http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

F. FABBRINI, *Fundamental Rights in Europe. Challenges and Transformations in Comparative Perspective*, Oxford University Press, 2014.

C. GRABENWARTER, *European Convention on Human Rights: Commentary*, Hart Publishing, 2014.

M. GLENNON, *National Security and Double Government*, Oxford University Press, 2014.

C. JACQUESON, *Union Citizenship and the Court of Justice. Something New under the Sun? Towards Social Citizenship* in *Eur. Law Rev.*, n. 3, 2002.

S. N. MALCOLM, *International Law,* University Cambridge Press, 7th Edition, 2014.

W. MOCK, *Human Rights in Europe: Commentary on the Charter of Fundamental Rights of the European Union*, Carolina Academic Press, 2010.

G. O' DONNELL, *Government Communications Headquarters (GCHQ): Baseline Assessment* in *Capability Reviews. Civil Service*, 2009.

A. REMIRO BROTÓNS, R.M. RIQUELME CORTADO, J. DÍEZ-HOCHLETITNER, E. ORIHUELA CALATAYUD, Y L. PÉREZ-PRAT DURBÁN, *Derecho Internacional*, Mc Graw Hill, 2007.

S. PEERS, T. HERVEY, J. KENNER, A. WARD, *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2014.

R. VAN DEN HOVEN VAN GENDEREN, *Cybercrime investigation and the protection of personal data and privacy* in *Economic Crime Division. Directorate General of Human Rights and Legal Affairs. Council of Europe,* 2008.