Esther Salamanca Aguado
Prof. Dr. University of Valladolid. Facultad de CC. Faculty of Social, Legal and Communication Sciences. Campus María Zambrano de Segovia.
E-mail: festher_salamanca@yahoo.com

- Submited: September 2014.
- Accepted: October 2014.

RESPECT FOR PRIVACY AND PERSONAL DATA PROTECTION IN THE CONTEXT OF MASS SURVEILLANCE OF COMMUNICATION

Abstract

The information leaked by Edward Snowden on the use by the United States and the United Kingdom of technologies that allow the indiscriminate collection of large amounts of data communications has caused great concern across Europe and has opened a debate on the impact of programmes of mass surveillance of communications on human rights. According to the case law of the European Court of Human Rights (ECtHR), such activities are an interference with the private lives of thousands of European citizens. This article analyses the guarantees that Article 8 of the European Convention on Human Rights (ECHR) provides for such interference and assesses whether these safeguards are sufficient in the case of extraterritorial surveillance. It also questions whether the Member States of the Convention are obliged to take measures to protect their citizens against surveillance contrary to the requirements.

KeyWords

Right to privacy, right to data protection, mass surveillance, positive obligations, national security

This work has been carried out within the framework of the research project: "El diálogo judicial multinivel en Espacio Europeo Multinivel: Las relaciones del TJUE con los tribunales constitucionales, el TEDH y otros tribunales internacionales" (DER 2012-36703) National Plan for R+D+Innovation (2004-2007), Ministry of Science and Technology. Principal researcher: Dr. José Martín y Pérez de Nanclares (University of Salamanca).

RESPECT FOR PRIVACY AND PERSONAL DATA PROTECTION IN THE CONTEXT OF MASS SURVEILLANCE OF COMMUNICATION

1. PROGRAMMES OF MASS SURVEILLANCE OF COMMUNICATION AND THEIR IMPACT ON THE EXERCISE OF HUMAN RIGHTS

At a time when the threat of new terrorist attacks looms over Europe, the implementation of secret surveillance programmes[1] aimed at countering terrorism and protecting national security have opened a global debate on their consequences for human rights[2] and demonstrated that in most States the regulatory frameworks are inadequate. Moreover, the routes towards the international protection of human rights such as the right to privacy and personal data protection are unclear, mainly because of the extraterritoriality component inherent in these activities.[3] It is a

1 We are referring to the surveillance programmes of the NSA (National Security Agency of the United States) and the GCHQ (Government Communications Headquarters of the United Kingdom): PRISM, XKeyscore, Bullrun, MUSCULAR, Tempora and Edgehill. For details of these programmes, see BOWDEN, C. *The US surveillance programmes and their impact on EU citizens' fundamental rights*, Study for the European Parliament, PE 474.405, Brussels: September 2013.

2 Much has been written on the subject of human rights protection while countering terrorism; see in particular, PÉREZ GONZÁLEZ, M., "Derechos humanos y lucha contra el terrorismo", A. Pastor Palomar (coord.), C. Escobar (dir.), Los derechos humanos en la sociedad internacional del siglo XXI, Madrid: Escuela Diplomática, 2009, pp. 39-62; COSTAS TRASCASAS, M., "Seguridad nacional y derechos humanos en la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) en materia de terrorismo internacional: ¿hacia un nuevo equilibrio?", E. Conde Pérez (dir.), Terrorismo y legalidad internacional, Madrid: Dykinson, 2012, pp. 187-207; CORNAGO PRIETO, N., "Lucha contra el terrorismo y derechos humanos", *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*, 2010, pp. 347-361; SHEININ, M. (coord.), "European and United States Counter-Terrorism Policies, the rule of law and Human Rights", *RSCAS Policy Papers 2011/03,* European University Institute, 2011; COUNCIL OF EUROPE, *Human Rights and the fight against terrorism: the Council of Europe Guidelines,* Strasbourg: Council of Europe Publishing, 2005.

3 See the conclusions of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Frank La Rue) in his *Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17 April 2013, A/HRC/23/40, and the reports of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Martin Scheinin), where it is highlighted that "the majority of counter-terrorism legislation activities since the events of 11 September 2001 have therefore focused on expanding Governments' powers to conduct surveillance", and that "States claim that since terrorism is a global activity, the search for terrorists must also take place beyond national borders, with the help

fact that States have never before had the capability to conduct simultaneous, invasive, targeted and broad-scale surveillance as they do today".[4]

After the initial revelations of Edward Snowden, former system administrator for the Central Intelligence Agency (CIA),[5] the special rapporteurs on the promotion and protection of the right to freedom of opinion and expression of the UN and the Organization of American States, in a joint declaration, "reiterate their concern at the existence of programs and security policies that could cause serious harm to the rights to privacy and to freedom of thought and expression" and "urge the corresponding authorities to amend the pertinent legislation and modify their policies in order to ensure that these programs measure up to international human rights principles".[6]

Following on the concerns of Member States of the UN at the negative impact of these surveillance practices on human rights, on 18 December 2013 the General Assembly adopted resolution 68/167, without a vote, on "the right to privacy in the digital age". In the resolution, which was co-sponsored by 57 Member States, the Assembly affirmed that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communication. It further called upon all States to review their procedures, practices and legislation related to communications surveillance, interception and collection

---

of third parties which potentially hold extensive amounts of information on individuals, generating a rich resource for identifying and monitoring terrorist suspects", A/HRC/13/37, 28 December 2009, paragraph 20. See also "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight", A/HRC/14/46, 17 May 2010, and "The Global Principles on National Security and the Right to Information" ("The Tshwane Principles") issued on 12 June 2013.

4 A/HRC/23/40, paragraph 33.

5 See the articles published in The Guardian and The Washington Post between June and August 2013 including, among others, "NSA collecting phone records of millions of Verizon customers daily", Glenn Greenwald, The Guardian, Thursday 6 June 2013; "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", Barton Gellman and Laura Poitras, *The Washington Post*, June 7, 2013; "NSA Prism program taps in to user data of Apple, Google and others", Glenn Greenwald and Ewen MacAskill, The Guardian, 7 June 2013; "UK gathering intelligence via covert NSA operation", Nick Hopkins, The Guardian, 7 June 2013; "GCHQ tapped fibre optic cables for data, says newspaper", The Guardian, 22 June 2013; "GCHQ taps fibre optic cables for secret access to world's communications", Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, The Guardian, 21 June 2013; "The legal loopholes that allow GCHQ to spy on the world", Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, The Guardian, 21 June 2013; "GCHQ: Inside the Top Secret World of Britain's Biggest Spy Agency", Nick Hopkins, Julian Borger and Luke Harding, The Guardian, 1 August 2013; "BT and Vodafone among telecoms companies passing details to GCHQ", James Ball, Luke Harding and Juliette Garside, The Guardian, 2 August 2013.

6 *Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression*, 21 June 2013, (available at **http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927&**).

of personal data, emphasising the need for States to ensure the full and effective implementation of their obligations under international human rights law.[7]

In the European Union, the disclosures made since June 2013 have raised serious concerns[8] and are particularly significant from a political and legal perspective.[9] The European Parliament (EP) approved a resolution on 4 July 2013 instructing its Committee on Civil Liberties, Justice and Home Affairs (LIBE) to conduct an in-depth inquiry into the matter.[10] In its report of 21 February 2014 ("The Moraes Report"), the LIBE Committee stated that there was compelling evidence of "the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the

7 "The right to privacy in the digital age", A/RES/68/167, 21 January 2014. See also the *Report of the Office of the United Nations High Commissioner for Human Rights*, "The right to privacy in the digital age", A/HRC/27/37, 30 June 2014, and AKRIVOPOULOU, CH. (ed.), *Human rights and risks in the digital era: globalization and the effects of information technologies,* Hershey, PA: Information Science Reference, 2012; KLANG. M, MURRAY, A. *Human rights in the digital age,* London; Portland, Or.; Glasshouse, 2005; DAVIS, F. *Surveillance, counter-terrorism and comparative constitutionalism,* Abingdon, Oxon: Routledege, 2014 (particularly pages 93 to 152).

8 See the report on the surveillance programme of the US National Security Agency, surveillance bodies in various Member States and their impact on EU citizens and transatlantic cooperation in Justice and Home Affairs. ("The Moraes Report") A7-0139/2014, 21.2.2014.

9 See the Declarations made on 10 June 2013 by the Vice-President of the European Commission, Viviane Reding, demanding explanations from the U.S. government for the PRISM programme and later declarations: "Mass surveillance is unacceptable – U.S. action to restore trust is needed now", 9 December 2013 (SPEECH/13/1048); "Protecting EU citizens' data from mass surveillance", 11 March 2014 (SPEECH/14/209). See also the declaration of the European Data Protection Supervisor (EDPS) on the need to rebuild trust between the U.S. and EU in data flows: "EDPS: Enforcing EU data protection law essential for rebuilding trust between EU-US", 21 February 2014 (EDPS/2014/04). And the *Report of 27 November 2013 on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection,* 16987/13, the communication from the European Commission on 27 November 2013: *Communication from the Commission to the European Parliament and the Council: Rebuilding trust in EU-UE data flows*, COM (2013) 846 final; *Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU, COM (2013) 847 final; Communication from the Commission to the European Parliament and the Council on the joint report from the Commission and the US Treasury Department regarding the value of TFTP provided data, COM (2013) 843 final. See also the 2013 Annual Report of the European Union Agency for Fundamental Rights,* Fundamental rights: challenges and achievements in 2013, the chapter entitled, "Information society, respect for private life and data protection", pp. 81 -100.

10 European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy, entrusted to its Committee on Civil Liberties, Justice and Home Affairs [P7_TA-PROV(2013)0322].

world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner".[11]

In its recommendations it calls on the EU Member States to prohibit blanket mass surveillance activities and to ensure that their national legislation and practices governing the activities of the intelligence services are in line with the standards of the European Convention on Human Rights and EU data protection legislation.[12]

The *Big Brother Watch and Others v. the United Kingdom*[13] was the first lawsuit brought before the European Court of Human Rights triggered by the information leaked by Edward Snowden, on use by the United States and the United Kingdom of technologies that enable the indiscriminate collection of vast amounts of communication data and the exchange of this data between the two States.[14] The applicants alleged that they are likely to have been the subject of generic surveillance by GCHQ and/or that the United Kingdom security services may have been in receipt of foreign intercept material relating to their electronic communications, such as to give rise to interferences with their rights under Article 8 of the ECHR.[15]

11 A7-0139/2014. (Main finding 1) It points specifically to US NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN), access to computer and telephone networks, and access to location data, as well as to systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), the decryption programme (Edgehill), the targeted 'man-in-the-middle attacks' on information systems (Quantumtheory and Foxacid programmes) and the collection and retention of 200 million text messages per day (Dishfire programme). Ibid. Finding 2.

12 *Ibid*. Findings 22, 23 and 27.

13 Application no. 58170/13 filed on 4 September 2013 and communicated to the UK government on 9 January 2014. The applicants are the British NGOs *Big Brother Watch*, *English Pen* and *Open Rights Group*, together with the German activist Dr. Constanze Kurz.

14 It specifically refers to the PRISM and TEMPORA programmes.

15 In the applicants' submission, there is no basis in domestic law for the receipt of information from foreign intelligence agencies. In addition, there is an absence of legislative control and safeguards in relation to the circumstances in which the United Kingdom intelligence services can request foreign intelligence agencies to intercept communications and/or to give the United Kingdom access to stored data that has been obtained by interception, and the extent to which the United Kingdom intelligence services can use, analyse, disseminate and store data solicited and/or received from foreign intelligence agencies and the process by which such data must be destroyed. In relation to the interception of communications directly by GCHQ, the applicants submit that the statutory regime applying to external communications warrants does not comply with the minimum standards outlined by the Court in its case law. The applicants further contend that the generic interception of external communications by GCHQ, merely on the basis that such communications have been transmitted by transatlantic fibre-optic cables, is an inherently disproportionate interference with the private lives of thousands, perhaps millions, of people, Fourth Section, Application no. 58170/13, Big Brother Watch

The aim of our work is not to conduct an in-depth analysis of this lawsuit or to anticipate the arguments that the ECHR is likely to put forward; it is to clarify what the minimum standards of protection are pursuant to Article 8 of the ECHR and whether these are adequate, given the new situation of mass surveillance of (national and extraterritorial) communications. We will first examine the scope of the right to privacy and personal data protection within this context, paying special attention to the cases in which the exercise of these rights can be limited. In other words, any interference with these rights must be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society. Secondly, we will assess whether ECHR Member States are obliged to take measures to protect their citizens against extraterritorial surveillance conducted by third countries that is contrary to the requirements of the ECHR.

2. RIGHTS GUARANTEED BY ARTICLE 8 OF THE ECHR

International human rights law not only recognises the right to privacy and family life as a fundamental human right,[16] it also regards it as a human right that supports other human rights and forms the basis of any democratic society.[17] Under the foregoing, each person is entitled to be protected against arbitrary or unlawful interference with his/her private and family life, his/her home and correspondence, as well as unlawful attacks on his/her honour and reputation. This right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. Therefore, the State is required to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks.[18]

---

and Others against the United Kingdom lodged on 4 September 2013. Statement of facts, (available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713#{"itemid":["001-140713").

16 In the Universal Declaration of Human Rights (Article 12), in the International Covenant on Civil and Political Rights (Article 17), in the Convention on the Rights of the Child (Article 16), the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (Article 14), in the American Convention on Human Rights (Article 11), in the European Convention on Human Rights and Fundamental Freedoms (Article 8) and in the EU Charter of Fundamental Rights (Article 7).

17 A/HRC/13/37, p. 6

18 Human Rights Committee, *General Comment 16*, paragraph 1. There are three requirements that determine the *right to respect for correspondence*. One, privacy of communications, i.e., individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself. Two, security of communications, meaning that individuals should be able to verify that their communications are received only by their intended

The development of information technology and enhanced computing power have enabled previously unimaginable forms of collecting, storing and sharing of personal data. Therefore, international core data protection principles have been developed to protect the right to privacy.[19] These principles include the obligation to obtain personal information fairly and lawfully; limit the scope of its use to the originally specified purpose; ensure that the processing is adequate, relevant and not excessive; ensure its accuracy; keep it secure; delete it when it is no longer required; and grant individuals the right to access their information and request corrections.[20]

Together with the fundamental right to privacy, the European system for the protection of human rights recognises the right to the protection of personal data and the ECHR has developed a well-established case law pursuant to Article 8 of the ECHR.[21]

2.1. The right to respect for privacy

Article 8 of the ECHR provides that everyone has the right to respect for his private and family life, his home and his correspondence. Where private life is concerned,[22]

recipients, without interference or alteration, and that the communications they receive are equally free from intrusion. And three, anonymity of communications, i.e., anonymity, if desired, allows individuals to express themselves freely without fear of retribution or condemnation. A/HRC/23/40, paragraph 23.

19 *General Comment* 16, "The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant", paragraph 10. See also, Council of Europe, Research Division. *Internet: case law of the European Court of Human Rights*, 2011.

20 See the OECD *Guidelines on the protection of privacy and transborder flows of personal data* (1980) and the *Guidelines for the Regulation of Computerized Personal Data Files* (adopted by General Assembly resolution 45/95 and E/CN.4/1990/72).

21 Articles 7 and 8 of the EU Charter of Fundamental Rights recognise respect for privacy and the protection of personal data as closely related but separate rights. In addition, Council of Europe Convention 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data was the first legally binding international instrument adopted in the field of data protection.

22 The ECtHR has repeatedly stated that the term "private life" is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with

Article 8 is given a broad interpretation by the ECtHR, seeing the notions of "private life" and "correspondence" as including communications by telephone, fax and email.[23] In addition, it has also ruled that information obtained through the monitoring of Internet usage,[24] the storage of data in a secret record and the disclosure of data pertaining to an individual's private life also come within the scope of article 8.[25]

The ECHR also provides the possibility to limit the exercise of this right in paragraph two of Article 8:

"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".

In the context of the interception of communications by intelligence services, the ECtHR holds that the power to secretly monitor citizens, characteristic of a police state, is only admissible, pursuant to the ECHR, when strictly necessary for safeguarding democratic institutions. In the case of *Klass and Others v. Germany*, the ECtHR recognised that a democratic state "should be able to secretly monitor subversive elements operating in its territory". And it also pointed out that the domestic legislature enjoys a certain but not an unlimited discretion in fixing the conditions under which the system of surveillance was to be operated, given that the Court, "being aware of the danger (…) of destroying democracy on the ground of

other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life", Case of Perry v. United Kingdom. Judgment of 17 July 2003, paragraph 36. See also the Case of Niemietz v. Germany. Judgment of 16 December 1992, paragraph 29; Case of Peck. v. United Kingdom. Judgment of 28 January 2003, paragraph 57. On the concept of private life, see in particular, Rubenfeld, J. «The Right of Privacy», Harvard Law Review, 1989, vol. 102, p. 737; De Schutter, O. «La vie privée entre droit de la personnalité et liberté», Revue trimestrielle des droits de l'homme, 1999, p. 827; Wachsmann, P. «Le droit au secret de la vie privé», in Sudre F.: Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme, Bruylant, 2005, p. 119, and Rigaux, F.: «La protection de la vie privée en Europe», in Le droit commun de l'Europe et l'avenir de l'enseignement juridique, by Witte B. and Forder, C., eds., Metro, Kluwer, 1992, p. 185.

23 Case of Liberty and Others v. United Kingdom. Judgment of 1 July 2008, paragraph 57. See also Weber and Saravia v. Germany. Judgment of 29 July 2006, paragraph 77; Case of Klass and Others v. Germany. Judgment of 6 September 1978, paragraph 41; Case of Malone v. United Kingdom. Judgment of 2 August 1984, paragraph 64; Case of Valenzuela Contreras v. Spain. Judgment of 30 July 1998, paragraph 64.

24 *Case of Copland v. United Kingdom*. Judgment of 3 April 2007, paragraph 41.

25 *Case of Rotaru v. Romania*. Judgment of 4 May 2000, paragraph 43; *Case of Leander v. Sweden*. Judgment of 26 March 1987, paragraph 48.

defending it, (…) Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measure they deem appropriate". Therefore, the Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse.[26]

In the instant case, the applicants (German nationals) did not dispute that the State had the right to have recourse to the surveillance measures contemplated by the legislation ("G 10");[27] they challenged this legislation in that it permits those measures without obliging the authorities in every case to notify the persons concerned after the event, and in that it excludes any remedy before the courts against the ordering and execution of such measures and thus violates Article 8. After examining the contested legislation and its interpretation by the German legislature, the Court agreed that some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention. In the context of Article 8, this means "that a balance must be sought between the exercise by the individual of the right guaranteed to him under paragraph 1 and the necessity under paragraph 2 to impose secret surveillance for the protection of the democratic society as a whole".[28] The ECtHR ultimately concluded that the German legislature was justified to consider the interference resulting from that legislation with the exercise of the right guaranteed by Article 8 as being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime.[29]

The German law allowing the secret monitoring of communications by the Federal Intelligence Service was again examined by the ECtHR pursuant to Article 8.[30] In the *Weber and Saravia v. Germany* case, the Court addressed for the first time what is known as "strategic monitoring" and the collection of personal data and its transfer to other authorities.[31] Firstly, it states that the mere existence of legislation which allows

26 *Case of Klass and Others v. Germany*. Judgment of 6 September 1978, paragraphs 42, 48, 49 and 50.

27 Act of 13 August 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications, enacted in pursuance of Article 10, paragraph 2 of the Basic Law (Grundgesetz).

28 *Case of Klass and Others v. Germany*, paragraph 59.

29 Ibid., paragraph 60.

30 "G 10" amended by the Anti-Crime Law, of 28 October 1994. On 29 June 2001, a new version of the G 10 Act came into force and the law of 1994 ceased to apply.

31 "Strategic monitoring is aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences (see in detail "Relevant domestic law and practice" below, paragraphs 18 et seq.). In contrast, so-called individual monitoring, that is, the interception of telecommunications of specific persons, serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed". *Case of Weber and Saravia v. Germany*, paragraph 4.

a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8.[32] This consideration is found again two years later in the case of *Liberty and Others vs. United Kingdom*[33] when the ECtHR had to judge whether British legislation of the 1990s, through the Electronic Test Facility ("ETF") which allowed the interception of 10,000 simultaneous telephone channels coming from Dublin to London and on to the continent, complied with the safeguards enshrined in Article 8.[34]

In both cases, the ECtHR examines - albeit with different outcomes – whether this interference is justified, in other words, whether it satisfies the requirements of paragraph 2 of Article 8: whether it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is "necessary in a democratic society" in order to achieve these aims.[35]

2.1.1. *In accordance with the law*

The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that "it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him and compatible with the rule of law".[36] In the special context of secret measures of surveillance, foreseeability

32 *Case of Weber and Saravia v. Germany*, paragraph 78. See also the Case of Klass and Others v. Germany, paragraph 41 and the *Case of Malone v. United Kingdom, paragraph* 64.

33 *Case of Liberty and Others vs. United Kingdom*. Judgment of 1 July 2008, paragraph 56.

34 During the period at issue in this application the relevant legislation was sections 1-10 of the Interception of Communications Act 1985 ("the 1985 Act"), which came into force on 10 April 1986 and was repealed by the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"). The 2000 Act came into force on 15 December 2000. The explanatory memorandum described the main purpose of the Act as being to ensure that the relevant investigatory powers were used in accordance with human rights. As to the first, interceptions of communications, the 2000 Act repealed, inter alia, sections 1-10 of the 1985 Act and provides for a new regime for the interception of communications.

35 Case of Weber and Saravia v. Germany, paragraphs 80 -138; Case of Liberty v. United Kingdom, paragraphs 58 – 70.

36 *Case of Weber and Saravia v. Germany*, paragraph 84. See, *inter alia*, the *Case of Kruslin v. France.* Judgment of 24 April 1990, paragraph 27; *Case of Huvig v. France.* Judgment of 24 April 1990, paragraph 26; *Case of Lambert v. France*. Judgment of 24 August 1998, paragraph 23; *Case of Perry v. United Kingdom*, paragraph 45; *Case of Dumitru Popescu v. Romania.* Judgment of 26 April 2007,

cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly; but, in order to avoid arbitrariness of the State and given the secret nature of the measures, "the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures".[37] Furthermore, "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".[38]

In its case law on the interception of communications, the ECtHR has developed the following minimum safeguards that should be set out in statute law: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed.[39] The ECtHR does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other,[40] and therefore applies them to situations created by the development of new surveillance technologies which in the British case allowed the interception of all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe. In fact, the UK Government accepted that, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication physically intercepted.[41] Moreover, the 1985 Act conferred a wide discretion on the State authorities as regards which communications, out of the total volume of those physically captured, were listened to or read.

The ECtHR recalls its case law to the effect that the procedures to be followed for examining, using and storing intercepted material, *inter alia*, should be set out in

paragraph 61.

37 Case of Weber and Saravia v. Germany, paragraph 93.

38 Case of Weber and Saravia v. Germany, paragraph 94.

39 *Ibid.*, paragraph 95.

40 Case of Liberty v. United Kingdom, paragraph 63.

41 *Ibid.*, paragraph 64.

a form which is open to public scrutiny and knowledge.[42] Furthermore, it pointed out that the German authorities stated that "the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order"; moreover, "the rules on storing and destroying data obtained through strategic monitoring" are set out in detail in the foregoing law. The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in some cases, had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications. In the opinion of the ECtHR, in the United Kingdom, extensive extracts from the Code of Practice issued under section 71 of the 2000 Act are now in the public domain, which suggests that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.[43]

In conclusion, unlike the *Weber and Saravia v. Germany* case, in the *Liberty v. United Kingdom* case, the Court did not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not "set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material". "The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law".[44]

To summarise, if we compare the application of the in accordance with the law requirement in the two cases, we can see why the ECtHR concluded that the impugned provisions of Germany's G 10 Act contained the minimum safeguards against arbitrary interference as defined in the Court's case law and therefore gave citizens an adequate indication as to the circumstances in which and the conditions on which the public authorities were empowered to resort to monitoring measures, and the scope and manner of exercise of the authorities' discretion,[45] while this was not the case with the UK Act.

42 *Ibid.*, paragraph 67.

43 *Ibid.*, paragraph 68.

44 *Ibid.*, paragraph 69.

45 Case of Weber and Saravia v. Germany, paragraph 101.

2.1.2. *Necessary in a democratic society*

The protection of national security is, according to paragraph 2 of Article 8, a legitimate aim that justifies interference with one's private life (secrecy of communications). However, it is not sufficient that governments invoke this aim, they must demonstrate that such interference is necessary in a democratic society in order to achieve these aims (necessary test) and proportionate to the legitimate aim pursued (proportionality test).[46]

In the *Weber and Saravia v. Germany* case, the ECtHR points out those national authorities enjoy certain discretion when choosing the type of surveillance system, but that contracting states do not enjoy an unlimited discretion, as established in the *Klass and Others* case. Nevertheless, the ECtHR must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse.[47] The German government argued that the monitoring measures based on the G 10 Act (after the 1994 amendment) had notably been necessary to combat international terrorism, while the applicants submitted that the scope of automatic surveillance under the amended G 10 Act was far too wide[48] and that the system of authorisation and supervision was inadequate.[49] After examining the German strategic monitoring system, the ECtHR found that there existed adequate and effective guarantees against abuses of the State's strategic monitoring powers, as was the case in the *Klass and Others* case. It was therefore satisfied that the respondent State, within its fairly wide margin of appreciation in that sphere, was entitled to consider the interferences with the secrecy of telecommunications resulting from the impugned provisions to have been necessary in a democratic society in the interests of national security and for the prevention of crime.[50]

46 Case of Klass and Others v. Germany, paragraph 49 and 50; Case of Weber and Saravia v. German, paragraphs 105 and 107.

47 *Case of Weber and Saravia v. Germany*, paragraph 106; Case of Klass and Others v. Germany, paragraphs 49 and 50.

48 *Case of Weber and Saravia v. Germany* "The Federal Intelligence Service was entitled to monitor all telecommunications within its reach without any reason or previous suspicion. Its monitoring powers therefore inhibited open communication and struck at the roots of democratic society. It was irrelevant whether or not it was already possible from a technical point of view to carry out worldwide monitoring (paragraph 111). "In the applicant's view, these wide monitoring powers did not correspond to a pressing need on the part of society for such surveillance" (paragraph 112).

49 *Ibid.*, paragraph 113.

50 Case of Weber and Saravia v. Germany, paragraph 137.

2.2. The right to the protection of personal data

According to the case law of the ECtHR, the protection of personal data falls within the scope of Article 8. The notion of "private life" is given a broad interpretation by the Court, and coincides with that of the *Council of Europe Convention 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data,*[51] the purpose of which is to "secure in the territory of each Party for every individual (…) respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (Article 1), with the latter being defined as "any information relating to an identified or identifiable individual" (Article 2).

In the *S. and Marper v. United Kingdom* case, the ECtHR pointed out that "the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (…)[52] and that "the subsequent use of the stored information has no bearing on that finding".[53] It went on to add that "in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained".[54]

In the instant case, the ECtHR noted that "(…) the fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals".[55] It also ruled that the storing by public authorities of data relating to the private life of an individual on the grounds of national security amounted to an interference with his right to respect for private life,[56] as did the storing of data relating to the private life of an individual obtained through the interception of telephone calls,[57] the protection of medical

51 *Case of Amman v. Switzerland*. Judgment of 16 February 2000, paragraph 65.

52 *Case of S. and Marper vs. United Kingdom*. Judgment of 4 December 2008, paragraph 67. See also the case of *Leander v. Sweden*. Judgment of 26 March 1987, paragraph 48,

53 *Ibid.* See also the *Case of Amman v. Switzerland*. Judgment of 16 February 2000, paragraph 69.

54 Ibid.

55 *Ibid.*, paragraph 68 and 86. See also the *Case of M.K. v. France*. Judgment of 18 April 2013, paragraph 26.

56 Case of Leander v. Sweden, paragraph 48. See also the case of Rotaru v. Romania, paragraph 43.

57 *Case of Amman v. Sweden*. Judgment of 16 February 2000, paragraphs 65, 69 and 80.

data,[58] the surveillance of an individual by GPS and the processing and use of the data obtained thereby,[59] the collection and storing of information on an individual's movements by car or air in a police database[60] and the registration of an individual as an "agent" in the files of a (former) State security agent.[61]

The ECtHR also held that "public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past";[62] "such information (studies, political activities and criminal record)", when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life" for the purposes of Article 8.1 of the Convention".[63] Furthermore, in the foregoing *Weber and Saravia* case, the Court takes the view that the transmission of data (collected by the intelligence services) and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted, constitutes a further separate interference with the applicants' rights under Article 8.[64]

Once it has been determined that Article 8 applies to the protection of personal data and the existence of interference in the enjoyment of this right, the ECtHR must investigate whether it satisfies the requirements of paragraph 2, i.e., whether the interference is in accordance with the law, pursues a legitimate aim and is necessary in a democratic society in order to achieve this aim.

2.2.1. *In accordance with the law*

As in the foregoing case, the ECtHR notes from its well established case law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal

58 *Case of L.H. v. Latvia*, Judgment of 29 April 2014, paragraph 56.

59 *Case of Uzun v. Germany*. Judgment of 2 September 2010, paragraph 52.

60 *Case of Shimovolos v. Russia*. Judgment of 21 June 2011, paragraph 66.

61 *Case of Turek v. Slovakia*. Judgment of 14 February 2006, paragraph 110.

62 *Case of Rotaru v. Romania.* Judgment of 4 May 2000, paragraph 43.

63 *Case of Rotaru v. Romania.* Judgment of 4 May 2000, paragraph 44.

64 *Ibid.*, paragraph 79

protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.[65] The level of precision required of domestic legislation depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed.[66]

The ECtHR has had the opportunity to apply these general principles to the Romanian law which authorises the Romanian Intelligence Service (SRI) to gather, store and make use of information affecting national security. In the *Rotaru v. Romania* case, the ECtHR had doubts as to the relevance to national security of the information held on the applicant. Nevertheless, it reiterated that it is primarily for the national authorities, notably the courts, to interpret and apply domestic law and noted that in its judgment of 25 November 1997 the Bucharest Court of Appeal confirmed that it was lawful for the RIS to hold this information as depositary of the archives of the former security services. That being so, the ECtHR concluded that "the storing of information about the applicant's private life had a basis in Romanian law".[67] As to the accessibility of the law, the ECtHR regards that requirement as having been satisfied, seeing that the law in question was published in Romania's Official Gazette on 3 March 1992.[68]

The "quality" of the legal rules relied on in this case must therefore be scrutinised by the Court, with a view, in particular, to ascertaining whether domestic law laid down with sufficient precision the circumstances in which the RIS could store and make use of information relating to the applicant's private life. The Court noted in this connection that "the aforesaid Law does not define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed. Similarly, the Law does not lay down limits on the age of information held or the length of time for which it may be kept".[69]

With respect to the existence of adequate and effective safeguards against abuse, the Court regards that in order for systems of secret surveillance to be compatible with Article 8 of the Convention: "they must contain safeguards established by law which

65 *Case of S. and Marper vs. United Kingdom*, paragraph 95. See also the *Case of Malone v. United Kingdom, paragraphs* 66-68; *Case of Rotaru v. Romania.* Judgment of 4 May 2000, paragraph 55; *Case of Amann v. Switzerland*. Judgment of 16 February 2000, paragraph 56.

66 *Case of S. and Marper vs. United Kingdom*. Judgment of 4 December 2008, paragraph 96. See also the *Case of Hassany Tchaouch v. Bulgaria*, paragraph 84.

67 Case of Rotaru v. Romania, paragraph 53.

68 *Ibid*., paragraph 54.

69 Case of Rotaru v. Romania, paragraph 56 – 58.

apply to the supervision of the relevant services' activities". This entails, *inter alia*, that "interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure".[70] In the instant case, the ECtHR noted that the Romanian system for gathering and archiving information did not provide such safeguards because the law provides no supervision procedure, whether while the measure ordered is in force or afterwards. That being so, the Court considered that domestic law did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. It concluded that the holding and use by the RIS of information on the applicant's private life were not "in accordance with the law", a fact that suffices to constitute a violation of Article 8.[71] In several later suits against Romania, the ECtHR re-examined these requirements and highlighted the absence of safeguards in its domestic law.[72]

2.2.2. *Necessary in a democratic society*

As indicated previously, in addition to the "in accordance with the law" requirement, the collection, use and storage of personal data must also pursue a legitimate aim and be necessary in a democratic society in order to achieve this aim. In the *Leander and Segerstedt v. Sweden* case, the ECtHR assesses whether an interference provided for by law is necessary in a democratic society in the interests of national security. The notion of necessity implies that the "interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued".[73] In this regard, the Court recognises that "national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved" and that "the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life".[74] The ECtHR stresses that within the wide margin of appreciation available to the State in the sphere of national security, "the Court must be satisfied that there exist adequate

70 *Ibid.*, *paragraph* 59. See also the *Case of Klass and Others v. Germany*, paragraph 55.

71 *Ibid.*, paragraphs 60 – 63.

72 See the Case of Dumitru Popescu v. Romania. Judgment of 26 April 2007; Haralambie v. Romania. Judgment of 27 October 2009; Association 21 of December 1989 and Others v. Romania. Judgment of 24 May 2011; Ioan Jarnea v. Romania. Judgment of 19 July 2011.

73 Case of Leander v. Sweden, paragraph 58.

74 *Ibid.*, paragraph 59.

and effective guarantees against abuse".[75] In the instant case, the Court reached the conclusion that the Swedish government "was entitled to consider that in the present case the interests of national security prevailed over the individual interests of the applicant", and that the interference to which the applicant was subjected "cannot therefore be said to have been disproportionate to the legitimate aim pursued".[76] The Swedish law that allows the intelligence service (Security Police) to store personal data in the name of the struggle against espionage and terrorism was re-examined in the *Segerstedt-Wiberg and Others* case.[77] In this case, however, the Court concluded that the storage of the information in the interests of national security was only necessary with respect to one of the applicants, but not for any of the remaining applicants.[78]

3. THE POSITIVE OBLIGATIONS OF THE STATE UNDER ARTICLE 8 OF THE ECHR

Article 8.2 of the ECHR sets out the cases in which interference, by public authorities, with the rights guaranteed under paragraph 1 are justified.[79] However, what happens when interference comes from third parties, be they private parties or States? In the context of mass surveillance of communications, the European Parliament has called on EU Member States:

"immediately to fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law".[80]

75 *Ibid.*, paragraph 60.

76 *Ibid.*, paragraph 67.

77 Case of Segerstedt-Wiberg and Others v. Sweden. Judgment of 6 June 2006, paragraph 87.

78 *Ibid.*, paragraph 92.

79 For more information on the contracting states' general obligations under the Convention, see FERNÁNDEZ SÁNCHEZ, P. A., *Las obligaciones de los Estados en el marco del Convenio Europeo de Derechos Humanos*, Ministerio de Defensa, Madrid, 1987.

80 The Moraes Report, paragraph 27.

Positive obligations involve the duty to ensure the effectiveness of the rights enshrined in the ECHR.[81] These obligations stem from a dynamic interpretation of the Convention, and it is the responsibility of the ECtHR to determine their existence and scope.[82] The ECtHR holds that, although the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities, there may in addition be positive obligations inherent in an effective respect for private and family life.[83] In the *Case of X and Y v. the Netherlands,* the Court recalls that Article 8 does not merely compel the State to abstain from such interference: "in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves".[84]

However, it is difficult to pinpoint when Article 8 calls for a State's positive obligation. In both contexts regard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole.[85] In the *Gaskin v. United Kingdom* case, the ECtHR believes that the question in each case was whether, regard being had to that margin of appreciation, a fair balance was struck between the competing interests, namely the public interest in this case in the efficient functioning of the child-care system, on the one hand, and the applicant's interest in having access to a coherent record of his personal history.[86] It further stated that "in striking this balance the aims mentioned in the second paragraph of Article 8 may be of certain relevance, although this provision refers in terms only to 'interferences' with the right protected by the first paragraph - in other words is concerned with the negative obligations flowing therefrom".[87] In practice, most of the cases brought before the ECtHR concern respect for family life, and the general

81 For more information on the contracting states' positive obligations under the ECHR, see, *inter alia*, FERNÁNDEZ SÁNCHEZ, P. A. *Las obligaciones de los Estados en el marco del Convenio Europeo de Derechos Humanos*, Madrid, 1987; PAVAGEAU, S. "Les obligations positives dans les jurisprudences de cours européenne et ineraméricaine des droits de l'homme", *Revista Colombiana de Derecho Internacional,* No. 6, julio-diciembre de 2005, pp. 201-246; XENOS, D. *The Positive Obligations of the State under the European Convention of Human Rights*, London and New York: Routledge, 2012.

82 PAVAGEAU, Stéphanie. "Les obligations positives…", *loc. cit.,* p. 206.

83 See, *inter alia*, the *Case of Johnston and Others v. Ireland*. Judgment of 18 December 1986, paragraph 55; *Gaskin v. United Kingdom*. Judgment of 7 July 1989, paragraph 38.

84 *Case of X and Y v. the Netherlands*. Judgment of 26 March 1985, paragraph 23.

85 *Case of Kroon and Others v. the Netherlands*. Judgment of 27 October 1994, paragraph 31; *Keegan v. Ireland*. Judgment of 26 May 1994, paragraph 21.

86 *Case of Gaskin v. United Kingdom*. Judgment of 7 July 1989, paragraph 40.

87 *Case of Gaskin v. United Kingdom*, paragraph 42.

interest of the community appears to prevail over this right, it being the individual's responsibility to prove that his particular interest predominates.[88]

There is no case law on the positive obligations of the State to secure respect for the privacy of its nationals against interference from third countries, and doctrine does not seem to envisage this possibility. Dimitris Xenos talks solely of the protection of individuals against acts of interference by private parties, including state actors when they act in a private capacity.[89] However, as stated previously, one of the characteristics of the mass surveillance activities carried out by the U.S. intelligence service is extraterritoriality.[90] Does this mean that if an act of interference is perpetrated by a State not acting as a private party, the territorial State that should have protected its citizens against this interference has no indirect responsibility in this regard? According to this interpretation, we would find ourselves in a situation of classical international law where the citizen is required to bring the case to the courts of a foreign State to exercise his rights, with all the difficulties that dealing with foreign intelligence services entails.[91] Or are we to assume that, up until now, there has been no evidence that would allow us to confirm the existence of this obligation of protection? In our opinion, a finalist and teleological interpretation of the ECHR would lead to the conclusion that ECHR Member States are obliged to take measures to guarantee the effective protection enshrined in Article 8 in relation to the mass surveillance of communications by third countries; which basically means that human rights should prevail over state sovereignty, an interpretation that has been used on other occasions.[92]

88 KILKELLY, Ú. *The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights*, Human Rights Handbooks, No. 1, p. 21.

89 201-246; XENOS, D. *The Positive Obligations of the State under the European Convention of Human Rights*, London and New York: Routledge, 2012.

90 See A/HRC/27/37, paragraphs 31-36.

91 "Several legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside, or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some point) and thus allow them to be collected and retained. The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens", A/HRC/27/37, paragraph 35.

92 In this respect, see PASTOR RIDRUEO, J. A.'s assessments in "La reciente jurisprudencia del Tribunal Europeo de Derechos Humanos: Temas escogidos", *Curso de Derecho internacional y relaciones internacionales de Vitoria-Gastéiz,* 2007, p. 251

4. CONCLUSIONS

In light of the ECtHR case law we studied, it cannot be denied that the programmes of mass surveillance of communications operated by intelligence services constitute an interference with the private lives of citizens. However, this interference may be necessary in a democratic society for countering international terrorism and protecting national security if the State offers adequate and effective guarantees against abuse. Such surveillance measures are only justified if they are provided for in domestic law, which must, in turn, respect the minimum human rights standards. In other words, the law governing mass surveillance systems should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and be compatible with the rule of law. By accessibility, we mean that domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures. Bearing in mind the risk of abuse inherent in any secret surveillance system, such measures must be based on a very specific law, particularly considering that technology is becoming increasingly sophisticated. Finally, domestic law must give the individual adequate protection against arbitrary interference, and include a supervision procedure.

However, in the digital age fundamental human rights, such as the right to respect for privacy and data protection, have to be seen from a new perspective. In the case of mass surveillance of communication which includes extraterritorial surveillance, interference with the exercise of the rights guaranteed under Article 8 of the ECHR may come from third countries. The guarantees required by the ECtHR case law appear to be adequate for domestic surveillance, but are difficult to apply to extraterritorial activities carried out by third countries. It is therefore necessary to take measures to ensure that secret mass surveillance activities are not conducted within a State unless they comply with the guarantees provided by its domestic law, particularly when you consider the different standards of protection that exist on the two sides of the Atlantic. On the other hand, the collection, use and storage, etc., of data by national authorities, obtained by foreign intelligence services, should be based once again on the domestic law of the receiving State, and provide the same guarantees as those required of the measures taken by the intelligence services themselves.

BIBLIOGRAPHY

AKRIVOPOULOU, CH. (ed.), *Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies,* Hershey, PA: Information Science Reference, 2012.

BOWDEN, C. *The US Surveillance Programmes and their Impact on EU Citizens' Fundamental Rights, Study for the European Parliament*, PE 474.405, Brussels, September 2013.

CORNAGO PRIETO, N., "Lucha contra el terrorismo y derechos humanos", *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*, 2010, pp. 347-361.

COSTAS TRASCASAS, M., "Seguridad nacional y derechos humanos en la reciente jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) en materia de terrorismo internacional: ¿hacia un nuevo equilibrio?", E. Conde Pérez (dir.), Terrorismo y legalidad internacional, Madrid: Dykinson, 2012, pp. 187-207.

COUNCIL OF EUROPE, *Human Rights and the fight against terrorism: the Council of Europe Guidelines,* Strasbourg: Council of Europe Publishing, 2005.

DAVIS, F. *Surveillance, counter-terrorism and comparative constitutionalism,* Abingdon, Oxon: Routledege, 2014 (in particular, pages 93 to 152).

FERNÁNDEZ SÁNCHEZ, P. A. *Las obligaciones de los Estados en el marco del Convenio Europeo de Derechos Humanos*, Ministerio de Defensa, Madrid, 1987.

KLANG, M, and MURRAY, A. *Human Rights in the Digital Age,* London; Portland, Or.; Glasshouse, 2005.

KILKELLY, Ú. The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights, Human Rights Handbooks, No. 1.

PASTOR RIDRUEO, J. A. "La reciente jurisprudencia del Tribunal Europeo de Derechos Humanos: Temas escogidos", *Curso de Derecho internacional y relaciones internacionales de Vitoria-Gastéiz,* 2007, pp. 240 – 276.

PAVAGEAU, S. "Les obligations positives dans les jurisprudences de cours européenne et ineraméricaine des droits de l'homme", *Revista Colombiana de Derecho Internacional,* No. 6, julio-diciembre de 2005, pp. 201-246.

PÉREZ GONZÁLEZ, M. "Derechos humanos y lucha contra el terrorismo", in A. Pastor Palomar (coord.), C. Escobar (dir.), *Los derechos humanos en la sociedad internacional del siglo XXI*, Madrid: Escuela Diplomática, 2009, pp. 39-62.

RIGAUX, F. «La protection de la vie privée en Europe», *in Le droit commun de l'Europe et l'avenir de l'enseignement juridique*, by Witte B. and Forder, C., eds., Kluwer, 1992.

RUBENFELD, J. «The Right of Privacy», *Harvard Law Review*, 1989, vol. 102, pp. 737 – 807.

DE SCHUTTER, O. «La vie privée entre droit de la personnalité et liberté», *Revue trimestrielle des droits de l'homme*, no. 40, octobre 1999, pp. 827-863.

SHEININ, M. (coord.), "European and United States Counter-Terrorism Policies, the rule of law and Human Rights", *RSCAS Policy Papers 2011/03,* European University Institute, 2011; COUNCIL OF EUROPE, *Human Rights and the fight against terrorism.*

WACHSMANN, P. «Le droit au secret de la vie privé», in Sudre F.: *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, pp. 119 – 156.

XENOS, D. *The Positive Obligations of the State under the European Convention of Human Rights*, London and New York: Routledge, 2012.