How Do Emergent Information Technologies In Counter-Terrorism Measures Affect Right To Privacy According To Article 8 Of The European Convention Of Human Rights?

Elif Mendos Kuşkonmaz

Introduction

Terrorism has been repeatedly linked with the threat to enjoyment of fundamental human rights. This is followed by encumbering states to adopt measures to counter terrorism and protect their citizens as well as society as a whole. The most efficient way to enhance security and counter terrorism has been believed to stay step ahead of the terrorists. This approach lead surveillance practices such as intelligence through communications and databases to be implemented. That said, surveillance practices also raises suspicions as they by all means go to the heart of right to privacy. Especially the very necessary secret nature of such measures creates a serious risk of arbitrary interference by states with many aspects of privacy including highly intimate aspects of the private sphere.

A closer look at these measures will show how they affect to our society because they shape and take the control of the behaviour of individuals. An individual will act differently if he feels that he is being watched.[1] This in turn enables the acceptance of a maximum security

[1] Paul de Hert, 'Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11' (September 2005) 1 Utrecht Law Review 67, 69.

society, where enjoyment of human rights comes under pressure.[2] So, are the human rights and security competing values and should we expect to give up on our rights for the pursuit of combating terrorism? This essay will be concerned with the question of whether responding to the threat of terrorism by means of surveillance measures is sufficiently scrutinized as a legitimate basis in respect of right to privacy. There appears to be a misconception stemming from the fact that concept of terrorism is being used too widely that it blurs the end of surveillance measures. However, it is the purpose and scale of such measures that distinguishes democratic regimes from police states.[3] If I were to jump to the argument of this essay, I would say that any surveillance measure must be sufficiently scrutinized in terms of collective human rights and democracy and thus a careful analysis of terrorism and national security must be assessed.

To support my argument I will focus on the fundamental human rights commitments and standards emerging from the European Convention of Human Rights[4]. In this regard, the essay will depart from identifying the types of state surveillance measures on combating terrorism which, under the Convention, are or should be the object of regulation and control. This brings the jurisprudence and transnational supervision of the European Court of Human Rights to the centre of this essay.[5]

---

[2] Garry T. Marx, 'Privacy and Technology' (January 1996) <http://web.mit.edu/gtmarx/www/privantt.html> accessed 12 April 2014.

[3] European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law' (2013) <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOLLIBE_ET(2013)493032_EN.pdf> accessed 12 April 2014, 3.

[4] Hereafter, the Convenion.

[5] Hereafter, the Court. Moreover, suffice it to note that the Convention is not the only supranational human rights instrument for protecting the right to privacy. For example, this right can also be found in the United Nation's International Covenant on Civil and Political Rights (i.e. ICCPR). However, it is the establishment of the Court makes the Convention more enforceable than those the ICCPR. Lee A. Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', (1998) 6 Int' J.L. & Info.

Taking this into account, I will examine the States' surveillance measures in the same way that the Court examines on a particular complaint. To begin with, the essay will define the scope of the right to privacy under Article 8 of the Convention. Furthermore, so as to distinct the actions which are relevant for the convention, the essay will examine what is an interference with the right to privacy. Finally, it focuses the key standards of determining legitimate restrictions on right to privacy under the Convention. Since the purpose of this essay is critically analyse the jurisprudence of the Court, the incident of excessive government spying and mass digital snooping will be left aside, but I believe that much will be discussed in the near future.[6]

I. The Scope of The Right to Privacy

Right to privacy under Article 8, obliges the States to protect four different interests.[7] These four main interests are namely, private and family life, home and correspondence and thus are connected with one another and some overlap.[8] However, for the purpose of this essay, we are particularly concerned with the definition private life.

In many of its judgements, the Court and formerly the Commission explicitly rejected an exhaustive descriptive definition of private life.[9] Hence, its case law is a starting point for some guidance as to the meaning

Tech. 247, 249.

6 Suffice it to note that after the disclosures surrounding PRISM and US surveillance programmes, Germany and Brazil submitted a draft resolution to the United Nations General Assembly. Following this, the United Nations committee that deals with human rights issue adopted the draft resolution. This draft resolution calls for an end to excessive electronic surveillance, data collection and other snooping techniques and therefore reaffirmes the right to privacy.

7 Stefan Sottiaux, *Terrorism and Limitation of Right The ECHR and the US Constitution* (Hart Publishing 2008) 267.

8 ibid.; Christopher Kuner *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 19.

9 *Niemitz v. Germany*, (1992) 16 EHRR 97, para. 29.

and the scope of private life for the purposes of Article 8.[10] In general, private life extends beyond the narrower meaning of privacy that puts an emphasis on the secrecy of personal information and seclusion.[11] In the Court's view, Article 8 protects a right to identity and personal development and the right to establish and develop relationships with other human beings and the outside world.[12] Therefore, interaction of a person with others, even in a public context, may fall within the scope of "private life".[13] For instance, in *Niemitz v. Germany*, the Court held that:

> "It would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, no reason why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world."[14]

Likewise in *Halford v. the United Kingdom*, the Court confirmed that the telephone calls made from business premises may be covered by the notion of "private life" in Article 8. In this regard, the Court used the notion of "reasonable expectation" for determining whether such calls falls within Article 8's protective ambit.[15] This notion was clarified by the Court in its subsequent judgments stating that a person's reasonable expectation of privacy "may be significant, although not necessarily con-

---

[10] Harris-O'Boyle-Warbirck, *Law of the European Convention on Human Rights*, (Oxford University Press 2009) 364.

[11] ibid.

[12] Bygrave (n 5) 256.

[13] *Uzun v. Germany*, App no 35623/05 (ECtHR 2 September 2010), para. 43.

[14] *Niemitz v. Germany* (n 9) para. 29.

[15] *Halford v. the United Kingdom* (1997) 24 EHRR 523, paras. 45-46.

clusive factor" to determine whether a person's private life is concerned by measures effected outside his home or private premises.[16]

In light of the above, we immediately see how difficult it is to make an account of a single concept of private life. The best way to overcome this difficulty is to focus on specifically identifying the interests and activities that the Court considered within the scope of private life.[17] In a nutshell, in the Court's voice, private life embraces the physical and psychological integrity of a person and sometimes embraces aspects of an individual's physical and social identity such as gender identification, name and sexual orientation and sexual life. Moreover, Article 8 also covers the right to develop relationship with other human beings even outside the domestic sphere.

II. Interference With Respect To Article 8(1)

The essential object of Article 8 has been expressed as protecting "the individual against arbitrary interference by the public authorities in his private or family life."[18] The Court did not develop an exhaustive definition of the notion of the interference or it did not specify its requirements.[19] In majority, the Court sought to establish an interference in a case-by-case approach.[20] Nevertheless, it is important to clarify the existence of an interference in order to distinct the actions which interfere with the Convention and which thus need to be justified from the activities that are not relevant to the Convention.

---

[16] *Uzun v. Germany*, (n 13) para. 44.

[17] Harris-O'Boyle-Warbirck (n 10) 365.

[18] *El Masri v. the Former Yugoslav Republic of Macedonia*, App no 39639/09 (ECtHR 13 December 2012), para. 248.

[19] Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice Towards Harmonised Data Protection Principles for Information Exchange at EU-level* (Springer 2012) 33.

[20] ibid.

Consequently, first we need to establish which measures taken by the public authorities constitute an interference with individuals' rights under Article 8 in order to assess violation of said article. After establishing the interference, the Court will further determine whether it is "in accordance with the law" and if so, whether any interference is "necessary in a democratic society" and proportionate to the legitimate aim pursued. This process will be examined in more detail in further chapter of this essay. Before examining this process, this section deals with establishing what types of activities have been held by the Court to amount to an interference within Article 8. The following examples of judgments should illustrate the Court's approach on what amounts an interference in the context of combating terrorism and serious crime.

A. Electronic Surveillance and Interception of Communications

Combating terrorism and serious crime strategies mainly cover secret surveillance of persons and interception of their communications.[21] The mere reading of Article 8 will not provide the question of what constitutes an interference. Hence, the following case law demonstrates what kind of State activities reveal an interference with right to privacy.

In its landmark decision in *Klass v. Germany* the Court dealt with the secret surveillance measures permitting state authorities to open and inspect mail and intercept telephone communications provided for under German legislation. In this decision the Court considered the mere existence of laws and practices that allow state agencies to carry out secret surveillance of citizens as being sufficient to interfere with citizens' rights under Article 8.[22]

Notably, the standards of electronic surveillance under Article 8 were developed in *Malone v. United Kingdom* and in the twin cases of

[21] Colin Warbrick, 'The Principles of the European Convention on Human Rights and the Response of States to Terrorism' (2002) 3 EHLR 287, 306.

[22] *Klass v. Germany* (1978) Series A, No 28, paras. 34-41.

Huvig and Kruslin v. France.[23] All these cases concerned with the interception of telephone conversations by police authorities. From these cases, *Malone v. United Kingdom* was about the "metering" of the applicant's telephone by the British telecommunications authority and disclosure of some information obtained from this practice to the police. The Court found that this disclosure made without the applicant's consent was an interference with the right to privacy. Moreover, the Court held that:

> "The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts … to an interference with a right guaranteed by Article 8."[24]

In its recent decision in *Liberty v. the United Kingdom*, the Court considered the interception of "external communications" under the Interception of Communications Act 1985 in the United Kingdom. Liberty and two Irish civil liberties organisations challenged the very broad powers to intercept electronic communications to and from the United Kingdom under the mentioned act. Here, the Court recalled its findings in previous cases stating that the mere existence of legislation which allows a system for the secret monitoring of communications entail a threat of surveillance for all to whom the legislation may be applied and this threat amounts in itself to an interference with Article 8. The Court further considered that the existence of powers granted to the authorities under the complained act particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants.[25]

---

[23] Sottiaux (n 7) 275. *Malone v. the United Kingdom* (1984) Series A, No 82; *Huvig v. France* (1990) Series A, No 176-B; *Kruslin v. France* (1990) Series A, No 176-A.

[24] *Malone v. the United Kingdom* (n 23) para. 84.

[25] *Liberty and Others v. the United Kingdom*, App no 58243/00 (ECtHR 1 July 2005), para. 56-57.

Another decision worth to mention here is *Weber and Saravia v. Germany*. In this decision the Court held another interference apart from the mere existence of legislation that allows secret monitoring of communications. According to the Court, "transmission of data to and use by other authorities" is an obvious interference with Article 8 and thereby this constitutes a "separate interference with the applicant's rights under Article 8".[26]

B. New Surveillance Technologies

The Convention is a "living instrument which should be interpreted according to present day conditions".[27] And it intends to guarantee "not rights that are theoretical or illusory but practical and effective".[28] This his interpretative method, surveillance technologies introduced by modern technologies the Court to consider the new surveillance technologies that introduce challenges to human rights even years after the Convention drafted. This dynamic interpretation and the Court's success in holding the challenges raised by the new technology will be illustrated below.

In light of the above, in *Uzun*, the Court more recently examined the compatibility of new surveillance techniques, namely Global Positioning System (i.e. GPS) with respect to right to privacy of people suspected of terrorist activities. In this case, the applicant, suspected of involvement in bomb attacks by a left-wing extremist movement, complained in particular that his surveillance via GPS and the use of the data obtained thereby in the criminal proceedings against him had violated his rights under Article 8. So as to examine whether the activity was interfered with the applicant's right to privacy, the Court considered if such data was the object of a compilation. Furthermore, the Court indicated the special features of this new surveillance technique stating that;

---

[26] *Weber and Saravia v. Germany*, (dec.) no 54934/00 (ECtHR 29 June 2006), para. 78.

[27] *Tyrer v. the United Kingdom* (1978) Series A. No 26, para. 31. Bygrave (n 5) 255.

[28] *Airey v. Ireland* (1979-80) 2 EHRR 305, para. 24.

"GPS surveillance by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feeling[29]."

Nevertheless, the Court considered that the investigative authorities systemically collected and stored data determining the applicant's whereabouts in the public sphere by the surveillance of him via GPS. Therefore such data was recorded to make further investigations and collect further evidence which was later used in the criminal trials against the applicant.[30] According to this consideration the Court held that the storage of data via GPS would amount to an interference with the right protected under Article 8.

C. Data Protection

Anti-terrorism strategies carry precisely several forms of data processing and inevitably genuine concerns over not only right to privacy but also data protection have been raised. So, where does the Court stand in respect of data protection? In the Court's view, data protection is an issue which falls within the scope of Article 8.[31] This is undoubtedly an important approach and solid source for existing data protection treaties.

To begin with, one should identify the concepts of data protection and privacy. The former is considered as a specific aspect of privacy that gives rights to individuals to control the processing of data about themselves.[32] Privacy is regarded as an independent and broader concept than data protection, but they overlap each other and are seldom distinguished.[33] Likewise, the Court recalled the close link between

---

[29] *Uzun v. Germany* (n 13) para. 52.

[30] ibid, para. 51.

[31] *Amann v. Switzerland*, App no 27798/95 (ECtHR 16 February 2000), para. 65; *Rotaru v. Romania*, App no 28341/95 (ECtHR 4 March 2000), paras. 42-43.

[32] Kuner (n 8) 19.

[33] ibid.

the two concepts.[34] That said, it was also held that not all aspects of the processing of personal data are protected by the Convention.[35] Here, the Court makes a distinction between personal data that falls within the scope of Article 8, unlike data protection in which the basic notion to be protected is "personal data" regardless of whether it relates to "private life" or not.[36] However, the Court in its several decisions tried to remedy this by applying a very broad interpretation of privacy and referring to existing data protection treaties in its numerous decisions.[37] Even though in its later decisions the Court may of the opinion that all personal data regardless of there relevance with individuals private life will be afforded the protection under the convention there also remains an open question whether or not the basic principles of data protection can be considered under Article 8.[38] For instance, the Court held that the rights under Article 8 do not imply the right to general access to data.[39] The Court does not

---

[34] Bygrave (n 5) 270; Hert (n 1) 75

[35] Hert (n 1) 75.

[36] ibid.

[37] ibid. For example, departing from assessing respect for life as "the right to establish and develop relationships with other human beings" the Court referred to Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data. *Amann v. Switzerland* (n 31) paras. 65-67; *Rotaru v. Romania*, (n 31) para. 43.

[38] Hert (n 1) 76.

[39] *Gaskin v. United Kingdom* (1989) 12 EHRR 36, para. 37. Also in *Leander v. Sweden*, the Court did not grant a general right to access to data for the applicant. See; *Leander v. Sweden* (1987) Series B, No 99. The Court in both cases, refrained its view of not granting a general right of access. However, *in Gaskin v. United Kingdom*, the Court concluded that the applicant had a vital interest in receiving the information that is the only concrete evidence of his childhood and understand his early development. The Court, further, held that since the Government has failed to grant him unimpeded access to that information, was in breach of its positive obligations under Article 8 and thus there has been a violation. See; *Gaskin v. United Kingdom*, para. 41. In this regard, the decisions in Leander and Gaskin are not analogous in respect of access to information. As for the latter, the Court considered the claim of access solely by reference to Article

explicitly deny this right, but it simply does not mention it.[40] Conversely, in data protection, the right to access is explicitly recognised.[41]

III. Compliance With Right To Privacy Under Article 8(2)

Right to privacy is not an absolute right. However, any state action that interferes with the right to privacy can only be compatible with the Convention within the limits specified in Article 8(2). Should this interference goes beyond these limits, then there will be a violation of the protected right under Article 8.

There are three main criteria Article 8(2) for an interference to be justified. The interference must be; (i) in accordance with the law, (ii) for one of the aims listed in the second paragraph, (iii) necessary in a democratic society. Accordingly, these criteria further presented below.

A. In Accordance With The Law

A key principle of the legality of an interference is that such interference by the public authorities must be "in accordance with the law". The Court, interpreted this principle in its early decisions in relation to the expression "prescribed by law" in Article 10.[42] The Court supported this conclusion by the fact that the two provisions overlapped in relation to freedom of expression through correspondence and the Court pointed out that not to give them an identical interpretation could lead to a different conclusion in respect of same interference. The Court further

8(2), namely to proportionality test. For more information see also; Bygrave, (n 5) 278, footnote 129.

[40] Hert (n 1) 74, footnote 39.

[41] ibid, 75.

[42] *Silver v. the United Kingdom*, (1983) Series A, No 61, para. 86.

observed that the word "law" in the phrase "prescribed by law" covers not only statute but also unwritten law.[43]

For an interference to be in accordance with law, it must have some basis in domestic law. However, the matter of "law" is not simply a formal inquiry. As a second step, the Court examines the "quality of law". This in turn requires that the law must be accessible, foreseeable and consistent with the rule of law.[44] To be more precise, in order to meet the requirement of accessibility, the law must be accessible to the citizens. As for the requirement of foreseeability, the law must be sufficiently precise to allow the person reasonably foresee its consequences[45]. The condition of compatibility with the rule of law, of law, therefore, implies along with the object and purpose of the Article 8 that domestic law in question must afford adequate legal protection against interferences by public authorities.[46] Where the domestic law does not provide safeguards against arbitrary use of power, it is accepted as being so defective that does not constitute law in the Convention's sense.[47]

In general, the tightness of the quality of law is linked to the seriousness of the interference in question.[48] For example, in the twin cases of *Huvig and Kruslin v. France* the legal authority for carrying out telephone tapping under a warrant was at issue. Here, the Court stated that interceptions of communications "represent a serious interference with private life and correspondence and must accordingly be based on a law that is 'particularly precise'. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated".[49]

---

[43] The Sunday Times *v. the United Kingdom*, (1979) Series A, No 30, para. 47.

[44] *Weber and Saravia v. Germany* (n 26) paras. 93-94.

[45] *Liberty v. the United Kingdom*, (n 25) para. 59.

[46] *Malone v. the United Kingdom* (n 23) para. 67.

[47] *Huvig v. France*, (n 23) paras. 34-35.

[48] Bygrave (n 5) 271.

[49] ibid., para. 32, *Kruslin v. France* (n 23) para. 33 (Emphasis added).

This being the case, the Court accepted a lower degree for the requirement of foreseeability in the context of secret surveillance.[50] The core of this view can be seen in *Malone* decision in which the government failed to convince the court that its power to intercept telephone conversations had a legal basis. At the relevant time, telephone tapping was regulated by administrative practice, the details of which were not published. The Court held that there was insufficient clarity about the scope or the manner in which the discretion of the authorities to listen secretly to telephone conversations was exercised; because it was an administrative practice, it could be changed at any time.[51] The Court, thus, concluded that the interception of communication did not satisfy the requirement of foreseeability on the ground that it was regulated only by administrative practice which lacked of clarity and was open to different interpretations. Having said that, the Court, before concluding its decision, observed the following;

> "The requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirements of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communication so that he can adapt his conduct accordingly".[52]

Nevertheless, the Court further relied on the risk of arbitrariness as being evident in the context of secret surveillance and held that the domestic law must be sufficiently clear in terms to give citizens an adequate indication as to the circumstance in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life

---

[50] Bygrave (n 5) 271.

[51] *Malone v. the United Kingdom* (n 23) para.87.

[52] ibid, para. 67.

and correspondence.[53] In this regard, even the requirement of foreseeability is interpreted more relaxed in the context of secret surveillance, this requirement still implies that the domestic law must be sufficiently clear as to require the question of when authorities may resort to secret surveillance.

Moreover, to the extent that a law confers a measure of discretion, it must indicate its scope and limits. According to the Court, the surveillance measures are not open to scrutiny by the individuals concerned or the public at large because of their very secret nature. For this reason, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power.[54] The law, therefore, must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities.[55]

Against this background, the Court listed a number of minimum safeguards for a domestic law in order to meet the requirements of quality of law. So as to list these safeguards, the Court regarded the foreseeability of the surveillance in particular.[56] These safeguards must be laid down in the domestic law can be summarised as follows;

> "A definition of the categories of people liable to have their telephones tapped by judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedures for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence and the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court".[57]

[53] ibid.

[54] ibid, para. 68.

[55] ibid.

[56] Sottiaux (n 7) 276.

[57] *Valenzuela Contreras v. Spain*, App no 27671/95 (ECtHR 30 July 1998), para. 46.

In light of the above, the requirement of foreseeability only to be fulfilled if each of the mentioned safeguards is included in the domestic law. However, it is pertinent to note that these decisions are related to the domestic law governing telephone tapping. Here, the question arises whether or not all other forms of secret surveillance have to comply with the abovementioned requirements. When considering other types of surveillance, the Court also referred to the telephone tapping cases. Having said that, it has not expounded on the safeguards that are required in those cases[58]. Consequently, according to the Court, "what is required by way of safeguard will depend, to some extent at least, on the nature and extent of the interference in question".[59]

B. Legitimate Aims

The Court and formerly established the Commission have rarely found a violation of Convention rights by reference to the legitimate aims that interference in question pursued.[60] The very reasoning of this approach can be explained by Member States' strong commitment and adherence to democratic governance and the protection of human rights[61] since it is highly unlikely that an accountable state wishes to be accused of expressly or implicitly incorporating arbitrary purposes into its legislation.[62] And yet, restrictive measures should be permissible in the framework of legitimate aims laid down in Article 8 (2). This, thus, includes the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or moral for the protection of the rights and freedoms of others.

---

[58] Sottiaux (n 7) 277.

[59] *P.G. and J.H. v. the United Kingdom* P.G. and J.H. v. United Kingdom App no 44787/98 (ECtHR, 25 September 2001) para. 46.

[60] Warbrick (n 21) 306.

[61] Yutaka Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR* (Intersentia 2002) 11

[62] ibid.

Since its decision in *Klass,* the Court accepted the public interest on combating terrorism and precisely in the case of secret surveillance in electronic means held it as a justifiable ground. It observed democratic societies as being threatened by highly sophisticated forms of espionage and by terrorism and therefore considered states to be able to implement the secret surveillance in order to counter such threats effectively.[63]. However, the Court further held that only under exceptional conditions secret surveillance practice should be accepted and it considered these conditions as being necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.[64] As we shall see below, national security and prevention of disorder or crime along with the responding to terrorist threats have been treated as the different sides of the same coin. However, if we look at the decision in *Klass*, we can say that the Court refers to espionage and terrorism separately when dealing with the question of national security. National security is a wider concept than prevention of terrorism, although the latter undoubtedly poses threat to the former. *Klass* illustrates that the Court put some weight to terrorism, but this is not to say that it is analogous with national security. Hence, it was also questioned whether the interest of national security and protecting the state against threats of terrorism are too broad and vague to meet the test of foreseeability.[65]

Precisely*, Kennedy v. the United Kingdom* is worth mentioning because it sheds a light on the Court's view on both national security and prevention of serious crime.[66] In this case, the applicant complaint that both terms, used in a British act to justify telephone tapping, were insufficiently clear. In view of the Court, the term national security complies with the foreseeability requirement since this requirement does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on "national

---

[63] *Klass and Others v. Germany* (n 22) para. 48.

[64] ibid.

[65] Sottiaux (n 7) 286-87.

[66] *Kennedy v. the United Kingdom*, App no 26839/05 (ECtHR 18 May 2010).

security" grounds.[67] By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance.[68] Moreover, additional clarification on how the term to be applied in practice has been provided by the Interception of Communications Commissioner. In this regard the Commissioner advocated that "it allows surveillance of activities which threaten the safety or well-being of the State and activities which are intented to undermine or overthrow Parliamentary democracy by political, industrial or violent means".[69]

By the same token, the Court found the reference to "serious crime" as being compliance with the foreseeability requirement if it is "further explained in the interpretative provisions of the contested act as well as in the act itself".[70] It concluded that "the reference to serious crime together with the interpretative clarifications in the Act, gives the citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures."[71] In brief, the Court interpreted the use of "national security" and "serious crime" together with clarifications made by the Commisioner's report for the former and within the Act itself for the latter. Regrettably, whether these terms seem to meet the foreseeability requirement without any clarifications remains an open question.

Although nothing explicitly stated for the concept of terrorism, the same can be said for this concept as well. In the meantime, an application was brought to the Court against mass surveillance activities carried out by GCHQ on September 2013[72]. The pending case concerns with the constitutionality of interception and data surveillance under the Tempora and PRISM programmes revealed by former NSA, United States intelligence agency, contractor Edward Snowden on 2013. This can be

---

[67] ibid, para. 159.

[68] ibid.

[69] ibid..

[70] ibid.

[71] ibid.

[72] *Big Brother and Others v. the United Kingdom* (Communicated Case) (App no 58170/13).

a unique opportunity for the Court to reassess the surveillance systems and terrorism.

C. Necessary in a Democratic Society

Provided that a measure restricting right to privacy is in accordance with the law, one could assume that there can be no objection. On the other hand, what if these laws are not compatible with the standards of democratic society? The answer lays within the fundamental objectives of law that is to protect liberties and rights. Although a measure restricting privacy would be foreseen by law and would be permissible by one of the legitimate aims laid down under Article 8 (2), this measure must still be "necessary in a democratic society".

Having said that, the Court is criticized as prefering to carry out the legality test rather than applying the democratic necessity test in order to establish the compatibility of surveillance measures.[73] As a way of illustration in *Malone*, the Court observed that the existence of some law granting power to intercept communications to aid the police in investigating and detecting crime "may be" necessary in a democratic society for the prevention of disorder or crime.[74] However, the Court concluded that since the interference in question was not in accordance with law, it did not have to examine further the content of the other guarantees required by Article 8(2).[75] In its latter decisions, the Court preserved its reluctancy to apply the necessity test for surveillance activities.[76]

The Court has examined the notion of "necessary in a democratic society" in the context of freedom of expression provided under Article 10.[77] The word "necessary" is not synonymous with "indispensable" nor

---

[73] Sottiaux (n 7) 278; Hert (n 1) p. 91.

[74] *Malone v. the United Kingdom* (n 23) para. 81 (emphasis added).

[75] ibid, para. 82.

[76] Hert (n 1) 80. *Huvig v. France* (n 23) para. 36; *P.G. and J.H. v. the United Kingdom* (n 59) para. 38.

[77] Hert (n 1) 59

does it have the flexibility of such expressions as "useful", "reasonable" or "desirable.[78] Therefore, the requirement for "necessary in a democratic society" can be broken down in to four parts. Is there a pressing social need for some restriction? If so, does the restriction in question correspond to that need? If so, is it a proportionate response to that need? In any event, are the reasons advanced by the authorities for the restriction "relevant and sufficient"?[79]

Although not explicitly stated in the Convention, the principle of proportionality plays a vital factor in respect of the Court's approach to the protection of human rights.[80] In a general framework, it has been considered as a fair balance between the protection of individual rights and the interests of the community at large. In this sense, a fair balance can be achieve only if restrictions on individual rights are strictly proportionate to the legitimate aim they pursue. The authorities are under the obligation to show that any interference with the protected rights does not go beyond what is strictly necessary to achieve the purpose.[81] Also, a measure could not be regarded as proportionate where another measure that is less burdensome measure on individuals' rights but equally capable of achieving the same objective exists.[82] Of particular importance with the implementation of surveillance measures for combating terrorism, it is likely to say that these measures are disproportionate especially when they are done on a mass scale since the extent of the interference is more stringent and runs counter to the values of a democratic society.

In assessing whether the measures taken by a State are "necessary in a democratic society", the Court held that national authorities enjoy a "margin of appreciation", particularly whether there existed a pressing

---

[78] *Handyside v. the United Kingdom* (1976) 1 EHRR 737, para. 48.

[79] Keir Starmer, *European Human Rights Law the Human Rights Act 1998 and the European Convention on Human Rights* (Legal Action Group 1999) 177.

[80] ibid, 169.

[81] ibid, 170.

[82] Arai-Takahashi (n 61) 62-63.

social need.[83] This allows the initial judgment of what sort of measures are necessary both in general and in particular cases to be determined to some extent by the national authorities.[84] However, this margin is subject to the European supervision.[85] Hence the Court adopted several principles to give some structures to its judgment whilst considering the exercise of the margin of appreciation by states such as the scope of this margin depends on the importance of the protected right, the character of democratic society and the interest to be protected by the interference nature and the seriousness of the interests at stake and the gravity of the interference.[86] It is the Court that determines whether the procedures for supervising the ordering and implementation of the measures restricting privacy are necessary in a democratic society.[87] Therefore, the exceptions provided under Article 8(2) have to be interpreted narrowly.[88]

After determining the scope of the margin of appreciation, whether it is wide or narrow, one may ask whether national authorities have overstepped this scope. In this regard, some authors argued that the requirement of proportionality should be applied for the relevant issue.[89] The question of proportionality of a measure in question means that a fair balance must be attained between the aim pursued and the rights of individuals. It is suggested that the application of proportionality principle can be regarded as the other side of this margin, serving as a corrective

---

[83] *Handyside v. theUnited Kingdom* (n 78) para. 48.

[84] Harris-O'Boyle-Warbrick (n 10) 349.

[85] European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law' (n 3) 31.

[86] Harris-O'Boyle-Warbrick (n 10) 351-59.

[87] *Kennedy v. the United Kingdom*, (n 66) para. 154.

[88] *Leander v. Sweden* (n 39) para. 67.

[89] F. Matscher, 'Methods of Interpretation of the Convention', in: R. St. J. Macdonald-F. Matscher-H. Petzold (eds.), The European System for the Protection of Human Rights (Martinus Nijhoff 1993) 63, 78.

and restriction of the margin of appreciation.[90] And thus, this principle should be used as to determine whether national authorities have exceeded their margin of appreciation.[91]

For the purpose of this essay it is pertinent here to examine the margin of appreciation allocated to States particularly in protecting national security and combating organised crime. As it was mentioned above, the scope of margin of appreciation varies depending on the circumstance of the case, the aim pursued and the particular nature of the interference. As far as protecting national security through secret surveillance measures are concerned, States enjoy a fairly wide margin of appreciation.[92] The reason why the Court accords this wide margin is assessed by reason of the serious threat being posed to the public order.[93] However, it is important not to lose sight of the fact that this width of margin would lessen as a result of thorough examination of some requirements that mentioned earlier in this section.

According to its several judgments the Court is prepared to accept the legitimacy of the fight against crime and terrorism.[94] In this regard, the Court observed the risk that a system of secret surveillance for the protection of national security poses and held that this system can undermine or even destroy democracy under the frond of defending it.[95] Therefore, states must provide adequate and effective guarantees against abuse.[96] In assessing these guarantees, all circumstances of the case should be considered such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities

---

[90] ibid.

[91] Arai-Takahashi (n 61) 15.

[92] *Weber and Saravia v. Germany* (n 26) para. 106.

[93] Warbrick (n 21) 287.

[94] R. A. Lawson and H.G. Schermers *Leading Cases of the European Court of Human Rights* (Ars Aequi Libri 1997) xxviii-xxix.

[95] *Klass v. Germany* (n 22) para. 48.

[96] Lawson and Scermers (n 94) xxviii-xxix.

competent to authorise, carry out and supervise them and the kind of remedy provided by the national law.[97]

By the same token, the Court took the view that States likely to face with more problems in investigating terrorist crime. In light of these reasons, it was asserted that accepting lower standards to justify the interferences in cases with investigating terrorist crime might be sufficient beyond those necessary for the investigation and prosecution of ordinary crime.[98] This might seem reasonable but a deeper look might be disturbing. Since the purpose of preventing terrorism has been introduced by states, this purpose has become a blanket excuse for mass surveillance of millions of individuals. And thus, the distinction between national security and terrorism has been blurred, the former being used beyond its natural meaning. Hopefully, the pending case against the Court concerned with the internet surveillance programmes operated by GCHQ might be a chance to re-assed the both concepts.

Conclusion

When confronted with terrorism, States may confront dilemma. They have the obligation to protect society and their citizens, but on top of that they must ensure that anti-terrorist measures fall within the existing human rights framework. Therefore, identifying terrorism as a key threat to their citizens and the society as a whole allow States to justify the development of surveillance practices. Some these forms of surveillance practices can be considered as quite legitimate in a democratic society, but their cumulative impact on individual's right to privacy is negative.

The European Court of Human Rights is prepared to accept the legitimacy of fight against terrorism and the need to take effective measures. Despite the absence of an agreed definition of terrorism, it has developed a jurisprudence on what constitutes an interference in the context of secret surveillance and information-gathering, which effec-

[97] *Weber and Saravia v. Germany* (n 26) para. 106.

[98] Warbrick (n 21) 307.

tively establishes a minimum safeguards for determining the lawfulness of secret surveillance. At the outcome, surveillance can more efficiciently be limited by relying on these set of criteria such as establishing a regime of independent supervision for the use of surveillance. The European Convention on Human Rights remains to be the solid framework for privacy protection in Europe and thus any surveillance practice that lacks of meeting the minimum standard laid down by the jurisprudence of the Court will not pass the Convention's test.

Bibliography

I. Books

Arai-Takahashi Y *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR* (Intersentia 2002)

Boehm F *Information Sharing and Data Protection in the Area of Freedom, Security and Justice Towards Harmonised Data Protection Principles for Information Exchange at EU-level* (Springer 2012)

Harris-O'Boyle-Warbirck *Law of the European Convention on Human Rights* (Oxford University Press 2009).

Kuner C *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013)

Lawson R.A. and Schermers H.G. *Leading Cases of the European Court of Human Rights* (Ars Aequi Libri 1997)

Matscher F 'Methods of Interpretation of the Convention',in: R. St. J. Macdonald-F. Matscher-H. Petzold (eds.), The European System for the Protection of Human Rights, (Martinus Nijhoff 1993)

Sottiaux S *Terrorism and Limitation of Right the ECHR and the US Constitution* (Hart Publishing 2008)

Starmer K *European Human Rights Law the Human Rights Act 1998 and the European Convention on Human Rights* (Legal Action Group 1999)

II. Articles

Bygrave LA 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', (1998) 6 Int' J.L. & Info. Tech 247

Hert, Paul de; 'Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11', (September 2005) 1 Utrecht Law Review 67

Warbrick C 'The Principles of the European Convention on Human Rights and the Response of States to Terrorism', (2002) 3 European Human Rights Law Review 287

III. E-Sources

European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law' (2013) <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOLLIBE_ET(2013)493032_EN.pdf> accessed 11 April 2014.

Marx, Garry T. 'Privacy and Technology', <http://web.mit.edu/gtmarx/www/privantt.html> January 1996, accessed 11 April 2014.

IV. Cases

Airey v. Ireland (1979-80) 2 EHRR 305

Amann v. Switzerland, App no 27798/95 (ECtHR 16 February 2000)

Big Brother and Others v. the United Kingdom (Communication Case) (Application No 58170/13)

El Masri v. the Former Yugoslav Republic of Macedonia App no 39639/09 (ECtHR 13 December 2012)

Gaskin v. the United Kingdom (1989) 12 EHRR 36

Halford v. the United Kingdom (1997) 24 EHRR 523

Handyside v. the United Kingdom (1976) 1 EHRR 737, para. 48

Huvig v. France (1990) Series A, No 176-B

Kennedy v. the United Kingdom App no 26839/05 (ECtHR 18 May 2010)

Klass v. Germany (1978) Series A, No 28

Kruslin v. France (1990) Series A, No 176-A

Leander v. Sweden (1987) Series B, No 99

Liberty and Others v. the United Kingdom App no 58243/00 (ECtHR 1 July 2005)

Malone v. the United Kingdom (1984) Series A, No 82

Niemitz v. Germany, (1992) 16 EHRR 97

P.G. and J.H. v. United Kingdom App no 44787/98 (ECtHR, 25 September 2001)

Rotaru v. Romania App no 28341/95 (ECtHR 4 March 2000)

Silver v. the United Kingdom (1983) Series A, No 61

The Sunday Times v. the United Kingdom (1979) Series A, No 30

Tyrer v. the United Kingdom (1978) Series A No 26

Uzun v. Germany, App no 35623/05 (ECtHR 2 September 2010)

Valenzuela Contreras v. Spain App no 27671/95 (ECtHR 30 July 1998)

Weber and Saravia v. Germany (dec.) no 54934/00 (ECtHR 29 June 2006)