

Stockholm University  
Faculty of Law  
Department of Law  
30 ECTS credits  
Fall 2008

# Privacy and Secret Surveillance from a European Convention Perspective

Author: Anders Lagerwall

## **Abstract**

A growing number of states are adopting wide-ranging surveillance programs on the basis of new security policy agendas. Concurrently, contemporary information technology has brought an increasing proportion of the private sphere under the global network umbrella. These developments place the delicate balance between privacy and national security on the edge. In this context, the European Convention has assumed a key role in the protection of privacy.

This thesis examines the Convention requirements on legality applicable to secret surveillance legislation. The exposition departs from the European Court's leading case law in order to identify and analyse the Convention's legality scheme and its impact on member states' surveillance programs. The thesis recognizes a correspondence between the magnitude of interferences and the level of protection required.

Although the Court appears to have acknowledged the technological development, it is arguable that the present employment calls for the next step in the Strasbourg's privacy practice. The thesis demonstrates how a combination of modern capabilities and traditional legal concepts may lead to an imbalance to the detriment of privacy.

Current legislative trends suggest that the boundary between national security and law enforcement blurs when states adopt broad surveillance programs. That tendency is a major challenge in the future protection of privacy.

## Table of contents

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	BACKGROUND	1
1.2	PURPOSE	4
1.3	METHODOLOGY	4
1.4	DEMARCATIION	5
1.5	DISPOSITION	6
<b>2</b>	<b>TECHNICAL ASPECTS</b>	<b>7</b>
2.1	THE POSITION OF SIGNALS INTELLIGENCE	7
2.2	DEFINITIONS USED	8
<b>3</b>	<b>INTRODUCING THE EUROPEAN CONVENTION AND PRIVACY</b>	<b>9</b>
3.1	THE EUROPEAN CONVENTION IN A SWEDISH CONTEXT	9
3.1.1	<i>Influence on the national legal system</i>	9
3.1.2	<i>National equivalents</i>	10
3.2	EUROPEAN CONVENTION AND PRIVACY PROTECTION	12
3.2.1	<i>Introducing article 8</i>	12
3.2.2	<i>Procedure for assessment</i>	13
3.2.2.1	Defining scope and interference	13
3.2.2.2	Is the interference legitimate?	15
<b>4</b>	<b>THE CONVENTION AND SECRET SURVEILLANCE</b>	<b>19</b>
4.1	THE SCOPE OF RIGHTS AND SECRET SURVEILLANCE	19
4.2	DOES THE SIA LEGAL FRAMEWORK CONSTITUTE AN INTERFERENCE?	19
4.3	SCOPE AND INTERFERENCE REGARDING ‘INCIDENTS’	22
<b>5</b>	<b>KEY CONVENTION REQUIREMENTS ON SECRET SURVEILLANCE</b>	<b>28</b>
5.1	RELEVANT CONVENTION REQUIREMENTS	28
5.2	THE LEGALITY CONDITION IN-DEPTH	30
5.2.1	<i>Requirements originating from the legality condition</i>	30
5.2.2	<i>Basis in national law</i>	32
5.2.3	<i>The quality of the law</i>	33
5.2.3.1	Purposes and distinctions	33
5.2.3.2	Executive summary of key case law	35
5.2.3.3	Accessibility	37
5.2.3.4	Foreseeability	41
5.2.3.5	Compatibility with the rule of law	47
<b>6</b>	<b>CONCLUDING REMARKS ON THE LEGALITY CONDITION</b>	<b>58</b>
6.1	SUMMARY OF CONCLUSIONS ON LEGALITY	58
6.2	SUGGESTED MODEL FOR APPLICATION	59
6.3	THE RATIONALE FOR LENIENT FORESEEABILITY	60
6.4	TECHNOLOGY – THREAT OR POSSIBILITY?	63
6.5	DEVELOPMENTS AND A GLIMPSE TO THE FUTURE	65

## Abbreviations

The following abbreviations are used in this thesis.

<i>Abbreviation</i>	<i>Description</i>
Commission	The European Commission on Human Rights
DS	Departementsserien (Ministry publications series)
European Convention	The Convention for the Protection of Human Rights and Fundamental Freedoms
European Court	The European Court of Human Rights
FRA	Försvarets radioanstalt (The Swedish National Defence Radio Establishment)
NJA	Nytt juridiskt arkiv 1 (Swedish Supreme Court Reports)
Prop	Proposition (Government bill)
SIA	The Signals Intelligence Act (2008:717)
SOU	Statens offentliga utredningar (Swedish Government Official Reports)

For information on Swedish legislation and descriptions of Swedish governmental and administrative functions in English, please refer to the “How Sweden is governed” service at the Government Offices website.<sup>1</sup>

---

<sup>1</sup> Government Offices of Sweden, at <http://www.sweden.gov.se/sb/d/575>, accessed on September 22<sup>nd</sup> 2008.

# 1 Introduction

## 1.1 Background

Technological development has brought possibilities to humanity which may have been unimaginable only a few decades ago. Means of communication, doing business and performing research and development have changed dramatically. Enhancements in terms of data transfer, processing capacity and storage is evident and constantly drives the development towards new fields of applications. Although the technological progress is accelerating, it is likely that the contemporary technology is not yet used at its peak capacity.<sup>2</sup>

The era of technological development and globalization of information has entailed a great impact on a number of judicial areas, of which privacy is one.<sup>3</sup> When Internet services like email, web browsing and file sharing are utilized, activities are continuously registered at different locations.<sup>4</sup> Other examples are storage of credit card transactions, mobile phone positioning and access control of various kinds. Registration of data is generally performed without the influence of the user.<sup>5</sup> Collectively these electronic footprints may provide very detailed charts of an individual.<sup>6</sup> Extensive data volumes and software advances facilitate the association of individuals with certain groups based on behaviour, preferences or activities.<sup>7</sup>

The altered prerequisite for states to perform intelligence operations is yet another consequence of technological development. Signals intelligence<sup>8</sup> has historically been conducted by intercepting ether transmissions, such as radio link, shortwave and satellite communication.<sup>9</sup> As the vast majority of contemporary communication is borne via cable media rather than ether media, states have argued that the value of traditional signals

---

<sup>2</sup> Waldo James, *Engaging privacy and information technology in a digital age*, National Academic Press, Washington D.C., 2007, pp. 88-97.

<sup>3</sup> For a chart and analysis on some contemporary privacy challenges, see SOU 2007:22, *infra* note 4, *passim*.

<sup>4</sup> SOU 2007:22, *Skyddet för den personliga integriteten - kartläggning och analys*, pp. 67-9.

<sup>5</sup> *Ibid.*

<sup>6</sup> *Ibid.*

<sup>7</sup> Waldo, *supra* note 2, p. 97.

<sup>8</sup> See definition in chapter 2.2.

<sup>9</sup> Prop. 2006/07:63, *En anpassad försvarsunderrättelseverksamhet*, pp. 57-8, and DS 2005:30, *En anpassad försvarsunderrättelseverksamhet*, p. 93.

intelligence has decreased dramatically.<sup>10</sup> The importance of signals intelligence is emphasised by the fact that it has been valued as the major raw material source for intelligence production.<sup>11</sup>

Several states have consequently enacted legislation that is either technology transparent or enables signals intelligence in cable media in order to adapt to the changed communication patterns.<sup>12</sup> It is also evident that an increasing number of states are expending further resources on signals intelligence targeting the global network.<sup>13</sup> The global network comprises communication in its entirety regardless of the technical media utilized.<sup>14</sup> Communication by means of Internet (email, chat, file sharing, web browsing, etc.), mobile and stationary telephony, facsimile and radio hence becomes the target of signals intelligence to a greater extent.<sup>15</sup>

The realignment of intelligence services is furthermore a consequence of a new security policy agenda. After the end of the Cold War, signals intelligence operations in the majority of Western-European countries have been characterised by the diminishing significance of traditional defence policy matters.<sup>16</sup> States, on the other hand, have adapted to a broader perception of the security policy agenda and the so-called new security threats.<sup>17</sup> Examples of new security threats are economic crises, proliferation of weapons of mass destruction, ecological threats, streams of refugees and migrants, and international crime and terrorism.<sup>18</sup> It is thus arguable that the targets of signals intelligence have expanded as the security policy agenda has broadened.

Why is this matter relevant for jurisprudence? As a mounting degree of privacy rests in the hands of the global network, states tend to adapt legislation to perform signals intelligence in that network. Many would agree that privacy is a human right worthy of protection. But

---

<sup>10</sup> Prop. 2006/07:63, *supra* note 9, p. 23, 57 and 60. According to the FRA, 98% of communications to and from Sweden is routed via cable medium, see SOU 2003:32, *Vår beredskap efter den 11 september*, p. 129. The Government Offices of Sweden estimate that 95% of all communication is transmitted via cable, at <http://www.sweden.gov.se/sb/d/10941>, accessed on September 20<sup>th</sup> 2008.

<sup>11</sup> DS 2005:30, *supra* note 9, p. 93, and prop. 2006/07:63, *supra* note 9, p. 57.

<sup>12</sup> E.g. prop. 2006/07:63, *supra* note 9, p. 60.

<sup>13</sup> SOU 2004:32, *Informationssäkerhet i Sverige och internationellt – en översikt*, p. 28.

<sup>14</sup> *Ibid.*

<sup>15</sup> DS 2005:30, *supra* note 9, pp. 94-6, and prop. 2006/07:63, *supra* note 9, p. 58.

<sup>16</sup> SOU 2003:30, *infra* note 18, p. 9, and prop. 2006/07:63, *supra* note 9, pp. 16-7.

<sup>17</sup> *Ibid.*

<sup>18</sup> SOU 2003:30, *Försvarets radioanstalt – en översyn*, p. 9.

to what extent can privacy be infringed by states in their justifiable pursuit of protecting civilians and combating crime? What components are weighed in the struggle to strike this balance? At this interface, the jurisprudence is brought to the fore to define the legal boundaries which outline the foundation for the politics of law.

But is this really a problem or just an academic issue? It has been argued that, in the aftermath of the September 11 terrorist attacks in the US, there has been a shift towards states bypassing the rule of law, and subjugating human rights concerns in the pursuit of national security policies.<sup>19</sup> Others have claimed that national security must be the priority, as this in turn protects civil liberties.<sup>20</sup> This tension accentuates the importance of a continuous legal dialogue on the position of human rights in the 21<sup>st</sup> century.

The enactment of the Swedish Signals Intelligence Act (SIA) in June 2008 and the ensuing debate illustrate that privacy and national security are subjects that may be problematic to unite.<sup>21</sup> A legal dimension to the debate is the issue of SIA compliance with the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention).<sup>22</sup> The subject was highlighted when a Swedish organisation lodged a complaint in July 2008 requesting the European Court to review whether the SIA violates the Convention.<sup>23</sup>

The matter of compliance is relevant not only in relation to Sweden's obligations under international public law towards other contracting states, but also due to constitutional requirements in the Instrument of Government, which explicitly declares that no act of law or other provision may be adopted that contravenes Sweden's undertakings under the

---

<sup>19</sup> Cameron Iain, *Brottsbekämpning, rättssäkerhet och integritet – vissa internationella trender*, SvJT, vol. 1, 2007, pp. 91-2, and Ramberg Anne, *Toångsmedel, rättssäkerhet och integritet - går det att förena?*, SvJT, vol. 1, 2007, p. 166.

<sup>20</sup> Davis Robert N., *Striking the balance: National Security vs. Civil Liberties*, Brooklyn Journal of International Law, vol. 29, no. 1, 2003, pp. 177-8.

<sup>21</sup> Enacted on June 18th 2008, the Swedish Parliament, at [www.riksdagen.se](http://www.riksdagen.se), accessed on September 22<sup>nd</sup> 2008, hereafter cited as 'SIA'.

<sup>22</sup> CETS 5, signed at Rome November 4<sup>th</sup> 1950, entered into force on September 3<sup>rd</sup> 1953, Council of Europe, [www.Conventions.coe.int](http://www.Conventions.coe.int), accessed September 22<sup>nd</sup> 2008, hereafter cited as 'European Convention'. See ch. 3.1 on the position of the European Convention in Sweden.

<sup>23</sup> Centrum för rättvisa, at <http://www.centrumforrattvisa.se/index.php/publisher/articleview/frmArticleID/23/>, accessed on September 18<sup>th</sup> 2008.

European Convention.<sup>24</sup> Further attention is drawn to this issue as the last year's developments imply a strengthened position for the Convention in the national context.<sup>25</sup>

This thesis departs from this position of the balancing of interests, and endeavours to shed light on European Convention requirements on legality applicable to the legislative frameworks which authorise means of secret surveillance, such as signals intelligence.<sup>26</sup>

## 1.2 Purpose

The purpose of this thesis is to identify and analyse European Convention requirements on legality applicable to secret surveillance legislation.

## 1.3 Methodology

A legal positivism viewpoint will be applied in the pursuit of accomplishing the purpose of this thesis. Consequently the sources of law studied are constitutional law, statutory law, case law, preparatory legislative materials (*travaux préparatoires*) and legal doctrine.

As to constitutional law, the Swedish Instrument of Government will be touched upon in order to review the significance of the European Convention from a national legislative perspective.

Relevant statutory law is the national legislation under review by the European Court and the SIA with its interrelated acts and ordinances. The SIA will not be the primary object of study. Rather it will be examined with the intention to illustrate relevant European Convention requirements. From a national context, the European Convention is classified under statutory law, as it has been incorporated into the Swedish legal system by parliamentary enactment.

The source of law of highest relevance is case law developed under the European Convention. Judgements passed by the European Court in the field of secret surveillance constitute the foundation upon which the analysis and conclusions of this thesis are based.

---

<sup>24</sup> The Instrument of Government (1974:152), chapter 2, article 23. See Fisher David I., *Mänskliga rättigheter – en introduktion*, second edition, Norstedts Juridik, Stockholm, 2001, pp. 80-2 on relevant international law aspects.

<sup>25</sup> See ch. 3.1.1.

<sup>26</sup> See ch. 2.2 in relation to definitions used.

Decisions originating from the Commission will primarily be addressed by reference to Court judgements.

The role of the preparatory work is primarily to provide background information on the tension between privacy and national security, and to illuminate the interpretation of statutory law. Legal doctrine is mainly used for background information purposes and to describe European Convention aspects of secret surveillance.

## **1.4 Demarcation**

The primary object of study is the European Convention requirements originating from article 8. Neither the Convention's legal status in national law nor its standing as a treaty are therefore of direct relevance. European law aspects other than those emanating from the European Convention will not be considered.

This paper does not attempt to provide a compliance assessment of the SIA legislative framework. Rather it brings to the fore certain SIA features in the course of elaborating on European Convention requirements. Swedish legislation other than the SIA will be discussed only insofar as necessary for the understanding of the subject.

To encompass all European Convention aspects in the field of secret surveillance is not viable in a study of this dimension. Accordingly the thesis intends to refer only the leading case law that resembles the characteristics of secret surveillance described in the SIA.<sup>27</sup>

In connection with the enactment of the SIA, the Swedish Parliament commissioned the Government to table a bill containing additional provisions on rule of law and supervision aspects.<sup>28</sup> A proposal referred for consideration was presented in December 2008.<sup>29</sup> As a result of the forthcoming changes, the SIA as of June 2008 will be discussed only to illustrate applicability and interference aspects.

---

<sup>27</sup> For definitions of secret surveillance and signals intelligence, see ch. 2.

<sup>28</sup> Parliament Defence Committee report, 200708:FöU15 Lag om signalspaning m.m.(förnyad behandling), at [http://www.riksdagen.se/Webbnav/index.aspx?nid=37&dok\\_id=GV01F%C3%B6U15](http://www.riksdagen.se/Webbnav/index.aspx?nid=37&dok_id=GV01F%C3%B6U15), accessed on September 30<sup>th</sup> 2008.

<sup>29</sup> Förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, at <http://www.regeringen.se/content/1/c6/11/80/70/6821847c.pdf>, accessed on January 20<sup>th</sup> 2009.

## **1.5 Disposition**

The second chapter briefly introduces the position of signals intelligence in the field of secret surveillance. Chapter three establishes relevant European Convention aspects and suggests a procedure for assessment. Scope and interference in the sphere of secret surveillance are discussed in chapter four. These aspects are illustrated by the characteristics of the SIA and European Court case law. Chapter five discusses the legality of interferences by identifying and analysing requirements originating from the Convention. The closing chapter presents concluding remarks based on the legality condition and presents a glimpse to the future.

## 2 Technical aspects

The purpose of this chapter is to introduce relevant technical terminology in order to place the relevant question of law in context.

### 2.1 The position of signals intelligence

Intelligence is produced from a number of different sources. Open sources that may be the object of examination are for example publications of different kinds or radio broadcasts. Covert sources of intelligence may be classified according to three categories: *imagery* intelligence, *human* intelligence and *signals* intelligence. Imagery intelligence involves aerial and space reconnaissance while human intelligence may be referred to as usage of secret agents.<sup>30</sup>

Signals intelligence is a generic term describing the interception and analysis of the intelligence gathering of signals.<sup>31</sup> The Swedish National Defence Radio Establishment<sup>32</sup> (FRA) employs two sub-categories of signals intelligence: *Communication signals intelligence* involves interception of both civil and military transmitted signals. *Technical signals intelligence* is directed at signals of purposes other than for communication, such as radar and navigation systems.<sup>33</sup>

From an interception point of view it is valuable to distinguish between the content of communications and incidents of communications.<sup>34</sup> The former is self-explanatory, referring as it does to the content of communication, for example the content of an electronic message. When a message is protected by encryption the use of cryptanalysis can potentially reveal the contents.<sup>35</sup>

---

<sup>30</sup> Encyclopædia Britannica Online, *Intelligence*, at [www.britannica.com](http://www.britannica.com), accessed on September 29<sup>th</sup> 2008.

<sup>31</sup> Ibid and Johnson Loch K., *America's Secret Power: The CIA in a Democratic Society*, Oxford University Press, Oxford, 1991, p. 41.

<sup>32</sup> In Swedish "Försvarets radioanstalt" or "FRA" in abbreviation.

<sup>33</sup> Prop. 2006/07:63, *supra* note 9, p. 22 and the FRA, at <http://www.fra.se/signalspaning.pdf>, accessed on October 8<sup>th</sup> 2008.

<sup>34</sup> C.f. Bignami Francesca, *European versus American Liberty: A comparative privacy analysis of antiterrorism data mining*, Boston College Law Review, vol. 48, no. 3, 2007, pp. 619-20. Incidents of communications will occasionally be referred to as 'incidents'.

<sup>35</sup> Encyclopædia Britannica Online, *Information theory*, at [www.britannica.com](http://www.britannica.com), accessed on October 8<sup>th</sup> 2008.

Incidents of communications, on the other hand, can be analysed to disclose structures of communication, for instance the parties, locations and frequency of communication.<sup>36</sup> This method is sometimes referred to as traffic analysis.<sup>37</sup> Traffic analysis can be performed even if the content of communications is encrypted.<sup>38</sup>

## 2.2 Definitions used

The notion of *secret surveillance* is well established in the European Court's case law and comprises a number of covert measures.<sup>39</sup> This thesis uses the term *signals intelligence* to refer to covert interception of signals, without technological or historical restraints, acknowledging that it constitutes one of many means of *secret surveillance*.<sup>40</sup>

Questions may arise regarding the relation to other notions in the field of secret surveillance, such as electronic eavesdropping, wire-tapping, bugging, monitoring and similar. Primary attention throughout this thesis is placed on the privacy impact pursuant to article 8 of the European Convention, rather than the technological methods applied. However, aspects of technology will be accounted for where appropriate for the object of the study.

---

<sup>36</sup> Another definition used is *traffic data*, c.f. chapter 1, article 1, para. d. in the "Convention on Cybercrime", CETS 185, signed at Budapest November 23<sup>rd</sup> 2001, entered into force July 1<sup>st</sup> 2004, Council of Europe, at [www.Conventions.coe.int](http://www.Conventions.coe.int), accessed October 10<sup>th</sup> 2008.

<sup>37</sup> *Supra* note 34 and *infra* note 151.

<sup>38</sup> *Supra* note 33, c.f. Johnson, *supra* note 31, p. 52.

<sup>39</sup> E.g. case of Liberty and others, *infra* note 60, para. 62, case of Weber and Saravia, *infra* note 89, paras 94 and 95, case of Klass and others, *infra* note 119, paras 36 and 75, and case of Malone, *infra* note 143, para. 68.

<sup>40</sup> C.f. Cameron Iain, *National Security and the European Convention on Human Rights*, Iustus Förslag, Uppsala, 2000, pp. 75-86.

### 3 Introducing the European Convention and privacy

The purpose of this chapter is to introduce the European Convention in a Swedish context and to acquaint readers with the Convention's key article on privacy.<sup>41</sup>

The chapter commences by briefly introducing the correlation between the Convention and the Swedish legal system, including the SIA. It then proceeds to describe the Convention's key privacy article from a practical viewpoint by suggesting an appropriate procedure for assessing a given case.

#### 3.1 The European Convention in a Swedish context

##### 3.1.1 *Influence on the national legal system*

Sweden was one of the first states to sign the European Convention after its establishment in the aftermath of the Second World War.<sup>42</sup> In 1995 the Convention was incorporated into Sweden's national legal system in the capacity of an act.<sup>43</sup> In addition, a constitutional provision was introduced in the Instrument of Government to emphasise the importance of the Convention.<sup>44</sup> This provision explicitly declares that no act of law or other regulation may be issued that contravenes Sweden's undertakings under the European Convention.<sup>45</sup> Hence European Convention elements should be essential components in the national legislative process.<sup>46</sup>

More than fifty years after ratification, the legal status of the Convention is still not fully clear in Sweden under the 'dualist state' structure.<sup>47</sup> Without endeavouring to elaborate this issue in its entirety, it is relevant to briefly consider the current standing of the Convention.

---

<sup>41</sup> This thesis concerns privacy provisions pursuant to article 8 of the European Convention, as it is the main privacy provision, see e.g. 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*, *Utrecht Law Review*, vol. 1, issue 1, 2005, pp. 70-3, and the thesis demarcation in ch. 1.4.

<sup>42</sup> Danelius Hans, *Mänskliga rättigheter i europeisk praxis*, third edition, Norstedts Juridik, Stockholm, 2000, p. 17.

<sup>43</sup> Prop. 1993/94:117, *Incorporering av Europakonventionen och andra fri- och rättighetsfrågor*, passim. The European Convention was incorporated by the act (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

<sup>44</sup> Prop. 1993/94:117, *supra* note 43, pp. 35-8.

<sup>45</sup> The Instrument of Government (1974:152), chapter 2, article 23.

<sup>46</sup> C.f. *supra* note 44.

<sup>47</sup> Cameron, *infra* note 56, pp. 174-7, Fisher, *supra* note 24, pp. 80-2, and Danelius, *supra* note 42, p. 18 and pp. 33-7.

The contemporary position suggests that the European Convention has obtained increasing importance in the national system as a result of recent judicial decisions. One such example is a verdict of 'not guilty' delivered by the Supreme Court, where a pastor was charged with a hate-speech crime with its basis in national criminal law. The court concluded that the defendant would be held 'guilty' pursuant to national law. However, since a verdict of guilty would likely have violated the freedom of speech protected by the Convention, the Supreme Court disregarded national law and ruled instead a verdict of 'not guilty'.<sup>48</sup>

A second example is a case of damage compensation due to erroneous deprivation of liberty. The Supreme Court held that compensation could be granted without a legal basis in national tort law, by reason of Sweden's obligations under the Convention.<sup>49</sup>

These precedent cases determined by the Supreme Court collectively suggest that higher judiciary bodies may be willing to acknowledge an effective Convention at the expense of national legislation.<sup>50</sup>

### 3.1.2 *National equivalents*

The protection granted by the Convention resembles regulations in the fundamental rights and freedoms catalogue expressed in the Swedish Constitution by the Instrument of Government.<sup>51</sup> Article 6 of the second chapter of the Constitution is a relevant privacy provision as it protects citizens against, inter alia, eavesdropping, recording of telephone conversations and other private communications. This protection can be restricted only by law and then only under certain conditions.<sup>52</sup>

Another constitutional safeguard is that a draft law which restricts the present privacy-provision may be held in abeyance for a minimum of twelve months if this is moved by at

---

<sup>48</sup> NJA 2005 s. 805, The Supreme Court, at [http://www.domstol.se/Domstolar/hogstodomstolen/Avgoranden/2005/Dom\\_pa\\_engelska\\_B\\_1050-05.pdf](http://www.domstol.se/Domstolar/hogstodomstolen/Avgoranden/2005/Dom_pa_engelska_B_1050-05.pdf), accessed on December 12<sup>th</sup>, 2008. For further analysis, see Österdahl Inger, *Åke Green och missaktande men inte hatiskt tal*, SvJT, 2006, pp. 213-26.

<sup>49</sup> NJA 2007 s. 295. For further analysis, see Schultz Mårten, *Skadeståndsrätten i de mänskliga rättigheternas tjänst*, JT, 2007/08, vol. 1, pp. 140-7.

<sup>50</sup> C.f. Danelius, *supra* note 42, pp. 36-7.

<sup>51</sup> For a general account, see Strömberg Håkan & Lundell Bengt, *Sveriges författning*, 19th edition, Studentlitteratur, Lund, 2004, pp. 84-95.

<sup>52</sup> The Instrument of Government, *supra* note 45, chapter 2, article 12.

least 10 Parliamentary members.<sup>53</sup> This mechanism was utilized in the drafting process of the SIA.<sup>54</sup>

The preparatory legislative materials to the incorporation act express that the constitutional rights and freedoms catalogue and the European Convention are to complement each other in the sense that the highest protection afforded by either instrument will apply.<sup>55</sup>

---

<sup>53</sup> Ibid, loc. cit., para. 3. The term 'safeguard' is interpreted as equivalent to legal protection.

<sup>54</sup> 200708;FöU15 Lag om signalspaning m.m.(förnyad behandling), *supra* note 28.

<sup>55</sup> Prop. 1993/94:117, *supra* note 43, p. 37.

## 3.2 European Convention and privacy protection

### 3.2.1 Introducing article 8

Article 8 of the European Convention obliges states to respect rights which fall under the notion of privacy.<sup>56</sup> The article provides:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being 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.

The first paragraph defines the protected rights, while the second sets out the conditions for when states may legitimately interfere with the exercise of rights.<sup>57</sup> The structure of article 8 hereby illustrates the Convention's inherent aim of striking a fair balance between individuals' exercise of rights and the necessity for states to impose measures for the protection of democratic society.<sup>58</sup> The European Court has stressed that the essential object of article 8 is to protect individuals against arbitrary action by public authorities.<sup>59</sup> An illegitimate interference by a public authority constitutes a violation.<sup>60</sup>

The Court has been reluctant to specifically define what each of the four rights in the first paragraph entails. On the other hand, the lack of precision has enabled the Court to develop case law that may take into account both social and technological developments.<sup>61</sup>

The case law originating from article 8 is diverse. The following subjects represent non exhaustive examples of what has been held in the realm of article 8: separation of children

---

<sup>56</sup> Cameron Iain, *An Introduction to the European Convention on Human Rights*, fifth edition, Iustus Förlag, Uppsala 2006, p. 111.

<sup>57</sup> Harris D J, O'Boyle M & Warbrick C, *Law of the European Convention on human rights*, Butterworths, London, 1995, hereafter cited as 'Harris et al.', p. 302 and pp. 283-301, c.f. *infra* note 63 on positive obligations.

<sup>58</sup> Case of Soering v. the United Kingdom, *infra* note 61, para. 89, see also case of Klass and others, *infra* note 119, para. 59.

<sup>59</sup> Case of Kroon and others v. the Netherlands, application no. 18535/91, para. 31.

<sup>60</sup> C.f. case of Liberty and others v. the United Kingdom, application no. 58243/00, paras 69-70.

<sup>61</sup> Harris et al., *supra* note 57, p. 303 and De Hert, *supra* note 41, pp. 73-7, c.f. case of Soering v. the United Kingdom, application no. 14038/88, para. 102.

by social authorities, prohibition on exercising profession or running a business, photographing in private environments, criminalisation of homosexual acts, registration of opinion, and environmental aspects of residence.<sup>62</sup>

Article 8 is also a source of positive obligations on states, which is inherent in the passage that grants the right *to respect for* each and every of the four rights. Illustrations of positive obligations are the requirements to make efforts to provide for the rights of an individual, and to protect against the actions of individuals that prevent the effective enjoyment of rights by other individuals.<sup>63</sup> This thesis pursues specifically European Convention requirements for legislation that authorises secret surveillance.<sup>64</sup> Hence the subject primarily falls under the notion of negative obligations, as it concerns the requirement on states to abstain from interfering with protected rights, rather than requirements to actively secure the effective enjoyment of rights.<sup>65</sup>

### 3.2.2 *Procedure for assessment*

The European Court has generally taken on a procedure for assessment that originates from article 8's structure.<sup>66</sup> This section endeavours to describe the fundamental elements of article 8 by adopting a similar procedure.<sup>67</sup>

#### 3.2.2.1 *Defining scope and interference*

The opening step when applying article 8 to the circumstances of a case is generally to define the scope of the right in question, which in practice implies an examination of the Court's case law. The present step hence seeks to define the legal sphere of the rights set out in the first paragraph of article 8.

Are there any limitations to the object of protection under article 8, such as acts of a criminal character? The European Court rejected a member state argument that the preparation of

---

<sup>62</sup> The case law in order: *Wallová and Walla v. Czech Republic*, application no. 23848/04, *Albanese et al. v. Italy*, application no. 1905/05, *Hannover v. Germany*, application no. 59320/00, *Modinos v. Cyprus*, application no. 15070/89, *Leander v. Sweden* *infra* note 208, *Guerra and others v. Italy*, application no. 116/1996/735/932. For further reading on the varied case law on article 8, see *Danelius*, *supra* note 42, pp. 301-54 and *Harris et al.*, *supra* note 57, pp. 305-20.

<sup>63</sup> *Harris et al.*, *supra* note 57, pp. 284-5 and 302-4, and *Cameron*, *supra* note 56, pp. 45-7.

<sup>64</sup> *C.f. Dutertre Gilles*, *Key case law extracts – European Court of Human Rights*, Council of Europe Publishing, Strasbourg, 2003, p. 241.

<sup>65</sup> *Harris et al.*, *supra* note 57, p. 284.

<sup>66</sup> *Ibid.*, p. 301.

<sup>67</sup> *Ibid.*, pp. 285 and 301. This approach also applies to the discussions in the following chapters.

crime fell outside the scope of article 8.<sup>68</sup> The Court stated that the interference of a phone call undoubtedly concerns the individual's right to respect for correspondence. It is therefore reasonable to argue that the Convention in this respect protects the rights as such, rather than the contents of the rights.<sup>69</sup> It is appropriate to point out that combating crime, which was the purpose of the interference in the referred case, may well be a legitimate aim for interfering with protected rights. However, the aim and necessity of an interference are subjects relevant to the subsequent legitimacy assessment, and does normally not deprive individuals of their rights under article 8.<sup>70</sup>

The subsequent step in an assessment is to examine whether the act of a state interferes with a right.<sup>71</sup> What signifies an interference? In general, an act by authorities that limits or rejects the enjoyment of a protected right constitutes an interference.<sup>72</sup> A failure to act may also constitute an interference in the course of positive obligations.<sup>73</sup>

It is for the applicant to establish an interference.<sup>74</sup> Admissibility requires that an individual can claim to be a victim of a violation by a member state.<sup>75</sup> Normally there is a verdict or a decision upon which the Convention compliance is questioned.<sup>76</sup> Consequently, individuals are normally unable to bring charges against particular legislation.<sup>77</sup> However, as a result of the potential secrecy of certain measures, the Court has developed conditions for when legislative frameworks may in themselves constitute interferences.<sup>78</sup>

The circumstances in the case of Kopp illustrate two cornerstones in this regard, namely the point in time for an interference and the importance of maintaining focus on the sequence of

---

<sup>68</sup> Case of A v. France, application no. 14838/89, paras 34-7.

<sup>69</sup> C.f. Harris et al., *supra* note 57, p. 320.

<sup>70</sup> Ch. 3.2.2.2, see however the Court's conclusion in case of Lüdi v. Switzerland, application no. 12433/86, commented by van Dijk et al, *infra* note 221, pp. 736-7.

<sup>71</sup> This overview disregards from the notion of 'incidental consequences' which does not reach a level of interference, c.f. Harris et al., *supra* note 57, pp. 320-1.

<sup>72</sup> C.f. case of Kopp, *infra* note 242, para. 5, case of Kroon, *supra* note 59, para. 40, and case of Segerstedt-Wiberg and others v. Sweden, application no. 62332/00, para. 73. See ch. 4.2 for a discussion on secret surveillance and interferences.

<sup>73</sup> Ch. 4.3.1.

<sup>74</sup> Harris et al., *supra* note 57, p. 335.

<sup>75</sup> The European Convention, *supra* note 22, article 34, formerly articles 25 and 46.

<sup>76</sup> *Infra* note 78.

<sup>77</sup> Case of Klass, *infra* note 119, para. 33.

<sup>78</sup> Case of Klass, *infra* note 119, paras 34-7, and Danelius, *supra* note 42, pp. 24-5. This matter is elaborated from an SIA perspective in ch. 4.2.

the procedure.<sup>79</sup> The Swiss Government, responding to accusations regarding telephone interception, questioned whether an interference had taken place since the received data had not been disseminated and subsequently destroyed.<sup>80</sup> The Court concluded that reasoning in relation to the ensuing use of intercepted data had no bearing on the finding of an interference.<sup>81</sup> Additionally, the Court has held that ‘a violation [i.e. an illegitimate interference] is conceivable even in the absence of any detriment’.<sup>82</sup>

By way of general observation, protected rights would not be of much worth if interferences could become legitimate once states chose not to proceed with their findings of secret surveillance. The above responding state’s positions are furthermore difficult to reconcile with the principles of foreseeability and the rule of law, which are elaborated below.<sup>83</sup>

### 3.2.2.2 *Is the interference legitimate?*

If the act of a state constitutes an interference, the next suggested step is to examine the *legitimacy* of the interference, which is the essence of the second paragraph of article 8.<sup>84</sup>

Accordingly, an interference is legitimate if it is:

- in accordance with law,<sup>85</sup>
- pursued with a legitimate aim, and
- necessary in a democratic society.<sup>86</sup>

The order of these conditions corresponds to the procedure of assessment applied in most cases of relevance for this thesis.<sup>87</sup> These three conditions have an exclusive effect, in the sense that a failure to comply with one condition constitutes a violation regardless of

---

<sup>79</sup> Case of Kopp, *infra* note 242.

<sup>80</sup> *Ibid*, para. 51.

<sup>81</sup> *Ibid*, para. 53. See also case of Rotaru, *infra* note 171, para. 46.

<sup>82</sup> Case of Huvig v. France, *application no. 11105/84*, para. 35.

<sup>83</sup> See ch. 5.2.3.5 for a discussion on the rule of law and article 8.

<sup>84</sup> The European Convention, *supra* note 22, article 8 paragraph 2. See also Harris et al., *supra* note 57, pp. 285-301 and pp. 335-53, and Cameron, *supra* note 56, pp. 105-10.

<sup>85</sup> Hereafter cited as the ‘legality condition’.

<sup>86</sup> The European Convention, *supra* note 22, article 8 paragraph 2. See Harris et al., *supra* note 57, p. 304 and pp. 344-53, and Cameron, *supra* note 56, pp. 107-10.

<sup>87</sup> C.f. case of Liberty and others, *supra* note 60, paras 58-9, case of Weber and Saravia, *infra* note 89, paras 80-137, and case of Klass and others, *infra* note 119 paras 43-60.

compliance with the other conditions. Once a violation is found it is redundant to continue the assessment.<sup>88</sup>

The legality condition (i.e. *in accordance with law*) entails requirements primarily aimed at the legal basis of the interference.<sup>89</sup> In the course of this thesis, the term 'legal basis' refers to the provisions that authorise the interference in question.

First, the legality condition requires that the interference has a basis in national law.<sup>90</sup> Regulations of different constitutional rank as well as case law generally qualify as such a basis. Hence the Court has adopted a relatively extensive view about the legal sources that may fall under the autonomous notion of 'law'.<sup>91</sup>

However, referring to the basis of an interference alone is not sufficient. As a second step, the legal basis is required to comply with three qualitative criteria in order to pass the legality condition. The qualitative criteria require the legal basis to be accessible, foreseeable and consistent with the rule of law.<sup>92</sup> If the Court concludes that the legal basis does not comply with any one of these requirements, the act is not legitimate and consequently constitutes a violation.<sup>93</sup> If the act complies with each of these three criteria, the Court proceeds to examine the following conditions.

The second condition in the legitimacy assessment is that interferences are to *pursue a legitimate aim*. Essentially this condition requires that interferences are justified for the protection of at least one of the following aims: national security, public safety or the economic well-being of the country, prevention of disorder or crime, protection of health or morals, and the protection of rights and freedoms of others.<sup>94</sup> It is important to note that the

---

<sup>88</sup> Cameron, *supra* note 56, p.105.

<sup>89</sup> C.f. case of Weber and Saravia v. Germany, application no. 54934/00, paras 80-102.

<sup>90</sup> Case of Weber and Saravia, *supra* note 89, para. 84, c.f. Cameron, *supra* note 56, p. 105, and Harris et al., *supra* note 57, pp.285-9 and pp. 338-43. This requirement is sometimes referred to as 'statutory basis in domestic law'. Since that definition is somewhat inconsistent with the conclusions drawn from the case law in question (*infra* note 91), it is hereafter referred to as 'basis in national law'.

<sup>91</sup> Case of the Sunday Times v. the United Kingdom, application no. 6538/74, paras 47-9, case of Barthold v. Germany, application no. 8734/79, para. 46, and Harris et al., *supra* note 57, pp. 285-9.

<sup>92</sup> Case of Weber and Saravia, *supra* note 89, paras 93-4. See ch. 5.2 for an elaboration on the subject.

<sup>93</sup> This was the case in Liberty and others, *supra* note 60, paras 69-70.

<sup>94</sup> Case of Weber and Saravia, *supra* note 89, para. 104 and Harris et al., *supra* note 57, pp. 289-90.

enumeration of aims is exhaustive.<sup>95</sup> Hence there are no grounds for interfering with the protected rights other than those explicitly articulated above.

The European Court has generally been reluctant to challenge the legitimate aim referred to by states.<sup>96</sup> Consequently, it has been argued that this condition is somewhat of a formality.<sup>97</sup>

The third and final condition in the legitimacy assessment is that the interference is *necessary in a democratic society*.<sup>98</sup> There is no static definition on what this passage implies, and it depends on the circumstances of each case, which is underlined by the Court's statement that necessity is neither synonymous with 'indispensable' nor 'reasonable'.<sup>99</sup>

The Court has granted national legislators and authorities applying the provisions in question a 'margin of appreciation' when determining the necessity of an interference.<sup>100</sup> The margin is not fixed and depends on the nature of the aim in question. For instance, national security has generally been granted a wide margin of appreciation.<sup>101</sup> The Court has nevertheless stressed that it has the final ruling, since the margin of appreciation goes hand in hand with supervision.<sup>102</sup>

The rationale for this separation is that national authorities, as distinct from the Court, generally possess adequate requisites to perform such judgements. The fact that the Convention is subsidiary to the national systems, rather than a final court of appeal, is another reason for the separation.<sup>103</sup>

---

<sup>95</sup> Case of Golder v. The United Kingdom, application no. 4451/70, para. 44.

<sup>96</sup> C.f. Weber and Saravia, *supra* note 89, para. 104, and case of Klass and others, *infra* note 119, para. 46. See also Harris et al., *supra* note 57, pp. 289-90 and pp. 343-4.

<sup>97</sup> Cameron, *supra* note 56, p. 105.

<sup>98</sup> The European Convention, *supra* note 22, article 8 paragraph 2, see Harris et al., *supra* note 57, pp. 290-301, and Cameron, *supra* note 56, pp. 107-10.

<sup>99</sup> Case of Silver and others, application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, para. 97, case of Handyside v. UK, application no. 5493/72, para. 48, Harris et al., *supra* note 57, p. 291, and Danelius, *supra* note 42, p. 305.

<sup>100</sup> *Ibid.* See also Cameron, *supra* note 40, p. 444.

<sup>101</sup> C.f. case of Leander, *infra* note 208, and case of Weber and Saravia, *supra* note 89, para. 106.

<sup>102</sup> *Supra* note 104.

<sup>103</sup> Danelius, *supra* note 42, pp. 48-9, and Cameron, *supra* note 56, p. 67 and pp. 107-10.

The notion of necessity implies both that interferences concurs with a pressing social need and is proportionate to the legitimate aim pursued.<sup>104</sup> While the doctrine of proportionality cannot be comprehensively accounted for in a thesis of delimited scope and length, some basic elements originating from the Court's case law may be briefly described; the measure must be capable of achieving the aims pursued, the least intrusive means should be applied, and there needs to be a reasonable balance between the exercise of a right on one hand, and the necessity of the legitimate aim on the other.<sup>105</sup>

This examination of necessity closes the legitimacy assessment.<sup>106</sup> A general procedure for applying article 8 has thus been elaborated.

---

<sup>104</sup> *Supra* note 99 and Ovey Clare & White Robin, *European Convention on Human Rights*, forth edition, Oxford University Press, Oxford, 2006, p. 232.

<sup>105</sup> Danelius, *supra* note 42, pp. 48-9, Harris et al., *supra* note 57, pp. 300-1, and De Hert, *supra* note 41, p. 80. See also case of Klass and others, *infra* note 119, para. 59.

<sup>106</sup> C.f. case of Klass and others, *infra* note 119, paras 44-5 and 60.

## 4 The Convention and secret surveillance

The purpose of this chapter is to apply the findings of the previous chapter within a secret surveillance context. Leading judgements from the European Court in combination with characteristics of the SIA legal framework will be used to illustrate scope and interference aspects.

### 4.1 The scope of rights and secret surveillance

The European Court case law is relatively rich in terms of its consideration of secret surveillance measures, such as signals intelligence and individual wire-tapping.<sup>107</sup> Despite that the Convention does not make reference to contemporary means of communication, the Court has found that telephony, facsimile and e-mail are covered by notions of *private life* and *correspondence* pursuant to article 8.<sup>108</sup> Additionally, the sphere of *private life* and *home* are not to be narrowly interpreted. Rather they may extend to both professional and business activities when the case concerns protection against arbitrary interferences by public authorities.<sup>109</sup> Legal doctrine furthermore suggests that forthcoming communication innovations will be considered by the Court under the notion of *correspondence*.<sup>110</sup>

This interpretation is commonly known as the 'dynamic charter of the Strasbourg case law'.<sup>111</sup> It has proven robust in the pursuit of interpreting the broadly defined rights in contexts drastically different from those that existed at the time the Convention was drafted.<sup>112</sup>

### 4.2 Does the SIA legal framework constitute an interference?

The following step, in accordance with the outlined process, is to determine whether the act of a state interferes with one or more protected rights. The act that illustrates this matter is the SIA legal framework that authorises signals intelligence. This question is approached by looking at the target of the secret surveillance in relation to the scope of the rights protected.

---

<sup>107</sup> See, inter alia, case of Klass and others, *infra* note 119, case of Malone, *infra* note 143, case of Weber and Saravia, *supra* note 89, and case of Liberty and others, *supra* note 60. See ch. 2.2 regarding definitions used.

<sup>108</sup> Case of Liberty and others, *supra* note 60, para. 56. For additional examples, see Sottiaux, *infra* note 244, pp. 275-6.

<sup>109</sup> Case of Niemietz v. Germany, application no. 13710/88, paras 29-32. See also the case of Halford, *infra* note 180.

<sup>110</sup> Harris et al., *supra* note 57, p. 320.

<sup>111</sup> De Hert, *supra* note 41, p. 74.

<sup>112</sup> *Ibid.*

The global network transmits communication in its entirety and hence comprises a wide range of services, such as stationary and mobile telephony, facsimile, email and other Internet-based communications.<sup>113</sup> The SIA legal framework targets the global network. It does so by instructing infrastructure providers owning transmission media to transfer signals that cross the border of Sweden to so-called 'interaction spots'.<sup>114</sup> An interaction spot refers to the site where data is handed over from the infrastructure provider to the FRA. The FRA is then responsible for transferring data from the interaction spots to the FRA.<sup>115</sup> The communications hence intercepted do primarily, but not exclusively, fall under the notions of *correspondence* and *private life*, which are afforded protection pursuant to article 8. Consequently, the SIA legal framework influences rights protected by the Convention and is therefore held in scope.<sup>116</sup>

It is axiomatic that each enumerated right in the article's first paragraph individually opens the doors to protection, whereas the legitimacy assessment in the second paragraph requires every condition to be fulfilled in order to avoid a violation.<sup>117</sup> Hence it is sufficient that the act of a state interferes with *one* of the enumerated rights for the restrictions in the second paragraph to apply.<sup>118</sup> Supplementary analysis on whether the SIA legal framework is in scope of *home* and *family life* is therefore rendered redundant.

It is concluded that the target of the signals intelligence pursuant to the SIA is in scope of the rights protected by article 8. But does SIA interfere with those rights? In what circumstances would such interference occur? The answers should be sought in the light of the act in question. Given the nature of signals intelligence as a measure of secret surveillance, it is generally not possible from an individual's point of view to know whether she or he is the subject of an interception.<sup>119</sup> Thus there is usually neither a verdict nor decision available against which to bring charges.<sup>120</sup>

---

<sup>113</sup> *Supra* note 15.

<sup>114</sup> Prop. 2006/07:63, *supra* note 9, pp. 72 and 83, and the Electronic Communications Act (2003:389) chapter 6 article 19 a.

<sup>115</sup> Prop. 2006/07:63, *supra* note 9, p. 85.

<sup>116</sup> Case of Liberty and others, *supra* note 60, para. 56, case of Weber and Saravia, *supra* note 89, para. 77, and case of Klass and others, *infra* note 119, para. 41.

<sup>117</sup> For an illustration of the former, see Case of A, *supra* note 68, para. 37, and case of Klass and others, *infra* note 119, para. 41.

<sup>118</sup> Case of A, *supra* note 68, para. 37.

<sup>119</sup> Case of Klass and others v. Germany, application no. 5029/71, para. 37.

The European Court has ruled that the mere existence of a legislative framework that authorises secret monitoring of communications causes a threat of surveillance for all those to whom the legislation may apply. The Court has concluded that this threat strikes at freedom of communications between the users of telecommunications services. Secret surveillance legislation therefore constitutes an interference pursuant to article 8, *regardless* of whether or not any measures have been taken against the applicant.<sup>121</sup>

The above exceptionally important conclusions by the Court entail that it is sufficient to establish that a monitoring system may *potentially* apply to an individual in order to threaten the enjoyment of a protected right and thus constitute an interference.<sup>122</sup> Accordingly the Court declared a complaint admissible where the applicant had conceivably been subject to secret surveillance, even though the state at the hearing retrospectively informed that no surveillance had taken place.<sup>123</sup>

What is the consequence of the possibility that an interference may be established at such an early stage? One effect is arguably that alleviating provisions *following* the interference have no obvious impact, since the interference is already established by the potential for a protected right to be threatened. That view would be amplified by the Court's correlated statement that subsequent use of intercepted information has no bearing on the finding of an interference.<sup>124</sup>

Given the case law regarding the scope and occurrence of interference, it is evident that the SIA legislative framework by its very design interferes with article 8.<sup>125</sup> This is not a matter of controversy, since the legislator clearly states this fact in the preparatory legislative materials.<sup>126</sup> That is, however, not to say that such interference constitutes a violation of article 8, which is a question of the legitimacy assessment.

---

<sup>120</sup> Cf. Danelius, *supra* note 42, pp. 24-7.

<sup>121</sup> Case of Liberty and others, *supra* note 60, para. 56, case of Weber and Saravia, *supra* note 89, para. 78, and case of Klass and others, *supra* note 119, para. 41. See also Danelius, *supra* note 42, p. 348.

<sup>122</sup> Case of Liberty and others, *supra* note 60, para. 57, and case of Klass and others, *supra* note 119, para. 41. C.f. Harris et al., *supra* note 57, p. 337.

<sup>123</sup> *Supra* note 119.

<sup>124</sup> *Ibid*, para. 53. See also case of Rotaru, *infra* note 171, para. 46.

<sup>125</sup> C.f. ch. 4.1, see also Cameron, *supra* note 40, pp. 91-7 for a technology-oriented approach on what is an interference with article 8.

<sup>126</sup> Prop. 2006/07:63, *supra* note 9, p. 88.

### 4.3 Scope and interference regarding ‘incidents’

Incidents of communications have previously been described as representing the structure of communication, i.e. the parties involved, frequency, location, point of time and so on.<sup>127</sup> This section elaborates on ‘incidents’ by assessing the SIA legal framework and case law from the European Court. The aim is to conclude the extent to which incidents gathered under SIA interfere with article 8.

The opening article of the SIA authorises signals intelligence within the boundaries of *defence intelligence operations* (DIO).<sup>128</sup> The concept is defined in a separate statute act, which stipulates that DIO shall be pursued to support Swedish foreign, security and defence policies, provided that it concerns foreign circumstances.<sup>129</sup> It is for the Government to confidentially decide on the alignment of the DIO.<sup>130</sup>

The opening article’s second paragraph enables the FRA to perform signals intelligence for other purposes, provided that it is *necessary* for the DIO.<sup>131</sup> These other purposes are, for instance, to develop technology and methodology, and to trace changes in the signals environment. According to the SIA preparatory legislative materials, *necessary* interception is performed for the needs of the FRA and does not generate any intelligence reports.<sup>132</sup> However the FRA Personal Data Act stipulates that information originating from *necessary* interception can be utilized as part of the DIO.<sup>133</sup> These two statements are potentially contradictory due to the difference in permitted use of information. This legal situation may furthermore blur the objective of the initial collection of the *necessary* interception and the demarcation in relation to the DIO.

The SIA and its interrelated statutory acts provide limited guidance as to the prerequisites and conditions for *necessary* interception. However the preparatory legislative materials stipulate that the interception normally excludes contents of communication, which is not

---

<sup>127</sup> Ch. 2.1.

<sup>128</sup> SIA, *supra* note 21, article 1 paragraph 1, the Defence Intelligence Operations Act (2000:130), article 1, and prop. 2006/07:63, *infra* note 9, p. 70. The legal definition is hereafter referred to as ‘DIO’.

<sup>129</sup> *Supra* note 128.

<sup>130</sup> Defence Intelligence Operations Act, *supra* note 128, article 1 paragraph 2, and SOU 2007:22, *infra* note 4, p. 243.

<sup>131</sup> SIA, *supra* note 21, article 1 paragraph 2.

<sup>132</sup> Prop. 2006/07:63, *infra* note 9, p. 72.

<sup>133</sup> Prop. 2006/07:46, *Personuppgiftsbehandling hos Försvarsmakten och Försvarets Radioanstalt*, pp. 67-8.

the case for DIO.<sup>134</sup> The below assessment consequently presupposes that *necessary* interception generates incidents of communication in accordance with the definition used.<sup>135</sup>

An additional key distinction between the DIO and *necessary* intelligence is that the latter is not bound to the statutory definition of DIO.<sup>136</sup> Consequently *necessary* intelligence may concern both Swedish and overseas circumstances, and is not tied to foreign, security or defence policy purposes. It is therefore arguable that the gathering of incidents under the SIA legal framework is relatively extensive, as it is not restricted by the limitations which apply for signals intelligence pursuant to DIO. On the other hand, *necessary* signals intelligence merely comprises incidents of communication, and not contents.<sup>137</sup>

Does the SIA interception of incidents interfere with the European Convention? The Convention does not provide direction on how to interpret the position of incidents in relation to the rights prescribed in article 8. Nor does the Court seem to have assessed incidents with similar characteristics as those of the SIA, although there is a relatively old decision which may shed light on this question.<sup>138</sup>

Before proceeding with the Convention aspects, a glimpse at two similar US cases may facilitate identifying the essential question. The first judgement was delivered by the U.S. Supreme Court in the late 1970's, and concerned the legality of electronic devices installed by the police to record dialling history. The Court held that the installation did not violate the protections pursuant to the Fourth Amendment<sup>139, 140</sup>. In the Court's findings, the Court held that 'we doubt that people in general entertain any actual expectation of privacy in the numbers they dial'.<sup>141</sup>

---

<sup>134</sup> *Supra* note 132.

<sup>135</sup> *Ibid*, cf. ch. 2.1. A definition of the data subject to *necessary* interception is arguably desirable, especially with regards to the legality condition elaborated in chapter 5.2.

<sup>136</sup> SIA, *supra* note 21, article 1 paragraph 1 e contrario, and prop. 2006/07:63, *supra* note 9, p. 72, 79 and 137.

<sup>137</sup> Cf. ch. 2.1.

<sup>138</sup> Case of Malone, *infra* note 143. As for foreign law, the German Basic Law article 10 protects both the contents of communication and 'circumstances of communication', e.g. time, frequency, sender, receiver and subscriber lines; see the German Federal Constitutional Court judgement, *infra* note 198, para. 161. See also the case of Valenzuela Contreras v. Spain, *infra* note 254, para. 47, and the case of P.G. and J.H. v. the United Kingdom, *infra* note 157, para. 42, which do not appear to deviate from the statements in Malone.

<sup>139</sup> Sottiaux, *supra* note 244, pp. 271-3.

<sup>140</sup> Smith v. Maryland, 442 U.S. 735 (1979).

<sup>141</sup> *Ibid.*, p. 742.

A relatively recent case from a high U.S. appellate court concerned the legality of government surveillance by means of collecting e-mail communication details, such as sender and receiver addresses, Internet Protocol (IP) numbers of visited websites and data volumes transferred. The appellate court held the circumstances analogous with the referred Supreme Court case, and the e-mail surveillance was therefore held to be lawful pursuant to the Fourth Amendment.<sup>142</sup>

Would these two cases be illustrative for the European Convention as well? The 25 year-old judgement in the case of *Malone* may suggest that the European Court has taken a partially different view when assessing the correlation between contents and incidents.<sup>143</sup> The surveillance method in question in *Malone* was similar to the U.S. Supreme Court example. A post office used an instrument named 'metering' to register the numbers dialled from a particular phone, including the time and duration of calls.<sup>144</sup>

In concluding on applicability the Court made a distinction between metering and intercepting contents of communications. Despite the distinction, the Court importantly held that numbers dialled is an integral element of communication and that metering therefore interfered with rights guaranteed by article 8.<sup>145</sup>

How does metering relate to the gathering of incidents of communications, as in SIA? Comparing the characteristics of *Malone* with the gathering of incidents in the SIA indicates that the methods are comparable, as they disclose patterns of communications. This essential resemblance suggests that incidents gathered under the SIA equally are within scope of the notions of *private life* and *correspondence*.<sup>146</sup>

Before concluding the assessment, it is appropriate to examine the differences featured between the SIA legal framework and the circumstances in *Malone*. Such examination should be based on a comparative analysis, taking into account aspects such as targeted means of communication and altered prerequisites for managing incidents data.

---

<sup>142</sup> United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

<sup>143</sup> Case of *Malone v. the United Kingdom*, application no. 8691/79.

<sup>144</sup> *Ibid*, para. 56.

<sup>145</sup> *Ibid*, para. 84. See also *P.G. and J.H. v. the United Kingdom*, *infra* note 157, para. 42.

As for the target of incidents under the SIA, it follows that the collected incidents may potentially comprise all communication means in the global network that cross the borders of Sweden.<sup>147</sup> This stands in clear contrast to the case of *Malone*, which targeted metering of telephony in the limited context of criminal investigation, with no reference to other means of communication.<sup>148</sup> It is therefore reasonable to argue that the SIA incidents by range exceed the interference magnitude confirmed in *Malone*. That finding furthermore indicates that all means of communication subject to the SIA interception are held within the scope of the Convention.

To what extent has data management capability changed in the time between the *Malone* judgement and the enactment of the SIA? And why is that relevant? Firstly, the European Court has made clear that the Convention is a living document that is to be interpreted in the light of contemporary conditions to render its rights practical and effective.<sup>149</sup> It is therefore reasonable to conclude that technological developments that may encroach on protected rights are to be taken into account in the analysis.

General challenges to privacy have previously been accounted for.<sup>150</sup> Of interest at this juncture are changes in the time span between the case of *Malone* and the SIA, with particular focus on how technological evolution for incidents may impact on privacy.

Contemporary capabilities enable examination of patterns of communications by means of traffic analysis and other software advances.<sup>151</sup> Not only is it possible to provide extensive charts of an individual's behaviour, but individuals may also be associated with other individuals or groups that share common characteristics.<sup>152</sup> Incidents of communication constitute the input, and hence the fundament for traffic analysis. This management of incidents may have an apparent impact on the notions of *private life* and *correspondence*.

---

<sup>146</sup> Ch. 4.2.

<sup>147</sup> Ch. 4.1.

<sup>148</sup> Case of *Malone*, *supra* note 143, para. 85.

<sup>149</sup> C.f. case of *Christine Goodwin v. the United Kingdom*, application no. 28957/95, para. 74, and case of *Rees v. the United Kingdom*, application no. 9532/81, para. 47.

<sup>150</sup> *Supra* note 3.

<sup>151</sup> For an overview of capabilities, see Acquisti Alessandro, *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton, 2008, pp. 95-112. See also *supra* note 2.

<sup>152</sup> Waldo, *supra* note 2, p. 97.

Furthermore, patterns of communications may reasonably reinforce interferences following the possible gathering of contents. This is because incidents provide a context to contents. An illustration of this is that fragments of contents may not be particularly valuable without access to information about the parties, the location and the means of communications utilized.

Another technological temporal distinction is the components constituting incidents. The metering mechanism employed in *Malone* gathered the numbers dialled, and the time and duration of phone calls from a particular telephone number.<sup>153</sup> That type of regulation brings a relatively clear separation between contents and incidents. However it is not possible to always maintain a similar separation, especially for Internet based communication.<sup>154</sup> For instance, web browsing normally generates incidents on visited web sites and search phrases utilized. These incidents expose the nature of the contents browsed by individuals, even though they are formally categorised as incidents.<sup>155</sup> The natural conclusion is hence that the notions of contents and incidents are merging along with technological development. It is therefore reasonable that the rationale for not granting equivalent protection to incidents decreases accordingly.<sup>156</sup>

The above comparisons suggest that the gathering of incidents under the SIA partially resembles the characteristics in *Malone*, for which the Court granted protection under article 8. The interference pursuant to the SIA is arguably broader, as it comprises incidents of all communication means in the global network rather than just telephony. Additionally, the SIA interference is substantial, as technological developments have brought software enhancements, which change the fundamentals for sustaining privacy.

Consequently there are strong reasons to suggest that the Court decision in *Malone* applies, *mutatis mutandis*, to all means of communications subject to interception under the SIA. Thus the incidents of communication gathered under the SIA are within scope of the

---

<sup>153</sup> Case of *Malone*, *supra* note 143, para. 83.

<sup>154</sup> Nicoll C., Prins J.E.J. & van Dellen M.J.M., *Digital Anonymity and the Law*, T M C Asser Press, The Hague, 2003, hereafter cited as 'Nicoll et al.', pp. 162-5.

<sup>155</sup> *Ibid.*

<sup>156</sup> Partly contra Cameron, *supra* note 40, pp. 105-6.

Convention and the collection arguably interferes with article 8.<sup>157</sup> Technological developments have accelerated the magnitude of the interferences in comparison with *Malone*. The legal consequence is that the interception of incidents pursuant to the SIA ought to be legitimate in order not to cause a violation. The preparatory legislative materials do not contribute to a different conclusion.<sup>158</sup>

---

<sup>157</sup> Another question is how the extent and nature of the interference impact the legality condition, see chs. 6.1 and 6.2; c.f. Cameron, *supra* note 40, p. 105 and the case of P.G. and J.H. v. the United Kingdom, application no. 44787/98, para. 46. The Court's reasoning herein suggests that information on dialling history from an individual's phone between two dates was 'strictly limited' in term of the *extent* of the interference. This judgement is not assumed to be representative for contemporary incidents of communications (or traffic data) in general, as it is limited in terms of communications means, target and time span. The lack of statutory basis on storage and destruction confirmed in para. 47 would be difficult to reconcile with the statutory requirement for the minimum requirements which were set out in latter case law, c.f. chs. 5.2.3.4 and 5.2.3.5.

<sup>158</sup> Prop. 2006/07:63, *supra* note 9, p. 88.

## 5 Key Convention requirements on secret surveillance

The aim of this chapter is to identify and analyse legality requirements of the European Convention necessary to accomplish the purpose of this thesis.

### 5.1 Relevant Convention requirements

The exercise of rights guaranteed in the first paragraph of article 8 may be subject to limitations. The assessment of the SIA legislative framework in the previous chapter illustrated that state acts may interfere with protected rights. When the Court finds an interference it will investigate whether such interference is legitimate according to the limitation clauses.<sup>159</sup>

To recapitulate, the purpose of this thesis is to identify and analyse European Convention requirements on legality applicable to secret surveillance legislation. What elements of the legitimacy scheme should be taken into account to accomplish the purpose?

Legitimacy requires the fulfilment of three conditions; namely that interferences are in accordance with law (i.e. legality), pursue a legitimate aim, and are necessary in a democratic society.<sup>160</sup> The 'legality condition' is evidently significant for the purpose of the study due to the impact on secret surveillance legislation.<sup>161</sup> However, what about the other two legitimacy conditions?

The legitimate aim condition merely has an indirect relation to the purpose.<sup>162</sup> It primarily refers to the aim, rather than the legality, of the interfering measure. The legitimate aim may additionally be regarded as somewhat of a formality, as it is rarely challenged by the Court; it is generally enough for states to refer to one of the aims.<sup>163</sup> For this reason there is no genuine interest in further elaborating the legitimate aim.

The third legitimacy condition requires interferences to be necessary in a democratic society. The necessity condition is not bound to the notion of legality, since it regularly takes

---

<sup>159</sup> Ch. 3.2.2.

<sup>160</sup> Ibid.

<sup>161</sup> Ch. 5.2.

<sup>162</sup> Ch. 3.2.2.2.

into account diverging aspects.<sup>164</sup> The case of *Leander* furthermore illustrates that Sweden as a respondent state successfully invoked a number of elements to the necessity assessment which were detached from the legislation that authorised the interference.<sup>165</sup> Thus, a comprehensive examination of the necessity condition would require studies beyond the impugned legislation, which is not achievable in a thesis of this delimited scope.

In conclusion, the purpose of this thesis primarily relates to the legality condition, which will thus be the object of study in the remaining exposition of the European Convention requirements.

---

<sup>163</sup> *Supra* note 96.

<sup>164</sup> Ch. 3.2.2.2.

<sup>165</sup> Case of *Leander*, *supra* note 116, paras 62 and 65, c.f., *mutatis mutandis*, the case of *Gorzelik and Others v. Poland*, application no. 44158/98, para. 96, and *Weber and Saravia*, *supra* note 89, para. 106. There may also be situations where one aspect may have an impact on more than one legality condition; see the case of *Klass and others*, *supra* note 119, para. 50 and ch. 5.2.3.5.

## 5.2 The legality condition in-depth

### 5.2.1 Requirements originating from the legality condition

Deriving from judgements passed by the European Court, the legality condition may be separated into two categories of requirements.<sup>166</sup> These categories respectively require:

1. That the interference has a basis in national law, and
2. That the basis holds certain qualitative criteria, namely it;
  - a. is accessible,
  - b. is foreseeable and
  - c. is compatible with the rule of law.<sup>167</sup>

The remainder of this chapter attempts to elaborate on the Strasbourg case law based on the above-suggested structure. Legal judgements do naturally have an inherent range of alternative interpretations, and the case law on secret surveillance would be no exception. Analysing the Court's legal reasoning in the pursuit of an underlying structure adds yet another level of complexity.

Despite the challenges, the sketched route may still be beneficial to the aims of the thesis. A structured display of the Court's requirements may provide for multifaceted compliance assessments and the possibility to approach questions of law from a number of perspectives. This is arguably the case regardless of the impracticality of providing for clear-cut delimitations at all times, especially as judgements are based on a variety of sources.

The below examination is mainly influenced by two cases delivered by the European Court, namely *Weber and Saravia* and *Liberty and others*.<sup>168</sup> These cases resemble the SIA legal framework to the extent that they concern secret surveillance of large amounts of data and

---

<sup>166</sup> Ch. 3.2.2.

<sup>167</sup> Similar assessment procedures are applied by the Court in, inter alia, case of *Weber and Saravia*, *supra* note 89, para. 84, case of *Liberty and others*, *supra* note 60, para. 59, and case of *Kruslin*, application no. 11801/85, para. 27. The requirements are reviewed in the order of the suggested structure.

<sup>168</sup> *Supra* notes 60 and 89 respectively. See also the executive case law summary in ch. 5.2.3.2.

are relatively up-to-date.<sup>169</sup> Furthermore these cases are valuable since they reconfirm an array of principles developed in cases featuring partially different circumstances.<sup>170</sup>

Several general aspects should be noted before embarking. With regards to interpretation, the Court has repeatedly indicated that article 8 paragraph 2, which encapsulates exceptions to the guaranteed rights currently accounted for, is to be narrowly interpreted.<sup>171</sup> Given that the below discussion on legality requirements derives from the limitations clause in article 8, the Court's interpretative statement should be kept in mind. Additionally, a set of general interpretative methods applied by the Court may also be relevant.<sup>172</sup>

The requirements and criteria comprising the legality condition have an exclusive effect, meaning that non-compliance with one requirement constitutes a violation regardless of the subsequent assessment.<sup>173</sup>

References to the European convention in general terms hereafter include the *acquis* of the convention, i.e. the convention along with the case law developed by the European Court.

---

<sup>169</sup> For the case of Weber and Saravia, *supra* note 89, paras 26, 88, 97 and 110. For the case of Liberty and others, see *supra* note 60, paras 5 and 57.

<sup>170</sup> Case of Liberty and others, *supra* note 60, para. 63.

<sup>171</sup> Case of Klass and others, *supra* note 119, para. 42, case of Silver and others, *supra* note 99, para. 97, and case of Rotaru v. Romania, application no. 28341/95, para. 47. See also van Dijk et al., *infra* note 221, p. 335.

<sup>172</sup> Cameron, *supra* note 56, pp. 71-3.

<sup>173</sup> Case of Kopp, *infra* note 242, para. 76, and case of Liberty, *supra* note 60, paras 60-9, and case of A, *supra* note 68, para. 39.

## 5.2.2 *Basis in national law*

The 'basis in national law' requirement is self-explanatory; it requires a basis for the state's interference of a protected right.<sup>174</sup> It does however not scrutinize the basis, which is the case for the 'qualitative criteria' in the next step.<sup>175</sup>

As previously observed, the Court has employed a broad approach to the notion of law. Written law of different constitutional rank as well as case law are comprehended.<sup>176</sup> This is also the case for public international law applicable in the national legal system in question.<sup>177</sup> The European Court has been reluctant to question the interpretation and application of law by member state courts.<sup>178</sup>

The 'basis in national law' requirement has attained relatively modest importance in secret surveillance cases before the Court in comparison with the 'qualitative criteria'.<sup>179</sup> The *Malone* proceedings however touched upon this aspect.<sup>180</sup> The case concerned the legitimacy of telephone interception and a method to collect incidents of communication called 'metering'.<sup>181</sup> While the telephone interception regulation was non-compliant with the rule of law, the Court concluded that metering was not subject to any national regulations except the mere absence of prohibition.<sup>182</sup>

The United Kingdom, in the capacity of respondent common law member state, argued that lacking a basis was legitimate as the interference was not prohibited in the UK and was hence lawful in the national system. The Court clearly rejected that argument by reference to the autonomous notion of law.<sup>183</sup> While flexible as to what legal sources may qualify as a

---

<sup>174</sup> Ch. 3.2.2

<sup>175</sup> C.f. case of Kopp, *infra* note 242, paras 61-3, and case of Liberty and others, *supra* note 60, para. 60.

<sup>176</sup> Ch. 3.2.2.2. For a discussion about the democratic impact of this approach, see De Hert, *supra* note 41, pp. 77-8.

<sup>177</sup> Case of Weber and Saravia, *supra* note 89, para. 87.

<sup>178</sup> Case of Huvig, *supra* note 82, para. 28, and Harris et al., *supra* note 57, p. 286.

<sup>179</sup> C.f. case of Liberty and others, *supra* note 60, para. 60, case of Klass and others, *supra* note 119, para. 43, and case of Weber and Saravia, *supra* note 89, para. 91. The conclusion applies to the cases of relevance for this thesis.

<sup>180</sup> Case of Malone, *supra* note 143. A case with similar characteristics on the 'basis in national law' is Halford v. the United Kingdom, application no. 20605/92, *passim*.

<sup>181</sup> *Ibid.* See also ch. 4.3.

<sup>182</sup> Case of Malone, *supra* note 143, para. 79 in relation to ch. 5.2.3.5.

<sup>183</sup> *Ibid.*, para. 87 and Cameron, *supra* note 56, p. 73.

basis, the Court nevertheless requires the existence of a basis.<sup>184</sup> Hence metering had no basis in national law and a violation was a fact on that ground.<sup>185</sup>

### 5.2.3 *The quality of the law*

After ensuring that there exists a basis for interfering with the right at stake, it is appropriate to proceed by examining the qualitative criteria developed by the Court. Consequently the assessment hereby shifts from merely identifying a national legal basis to a thorough examination of the provisions in question to determine compliance with the qualitative criteria.<sup>186</sup>

#### 5.2.3.1 *Purposes and distinctions*

As previously indicated, this thesis suggests a structure which distinguishes between the three qualitative criteria.<sup>187</sup> Rather than discussing similarities and differences individually, this opening section endeavours to briefly outline key characteristics and suggest distinctions to facilitate the forthcoming discussion. Each qualitative criterion will then be further elaborated in separate sections.

To begin, the accessibility criterion requires the legal basis to indicate the provisions applicable to a given case. This is normally achieved by means of publication. Accessibility may be classified as a formal criterion as it does not set out requirements aimed at the substantial provisions but rather obliges provisions to be made available. On the contrary, the foreseeability and rule of law criteria entail requirements to be accounted for in the legal basis.<sup>188</sup>

In the field of secret surveillance, foreseeability does not imply that individuals should be able to foresee when authorities are likely to have recourse to secret surveillance measures, so that they can adapt their behaviour accordingly. Rather, foreseeability in this context means that the legal basis should be sufficiently clear to give individuals adequate indication regarding the circumstances and conditions under which authorities may resort

---

<sup>184</sup> Ch. 3.2.2.2. This conclusion may potentially disclose the different legislative cultures between civil law and common law member states, demanding explicit basis in the national legal system, see De Hert, *infra* note 41, p. 73.

<sup>185</sup> Case of Malone, *supra* note 143, paras 83-7 and 56.

<sup>186</sup> C.f. Rotaru, *supra* note 171, para. 56, case of Huvig, *supra* note 82, paras 30-1, case of Weber and Saravia, *supra* note 89, paras 93-5, and case of Volokhy v. Ukraine, application no. 23543/02, para. 50.

<sup>187</sup> Ch. 5.2.1.

to secret surveillance. Foreseeability consequently refers to the question about *when* authorities may resort to secret surveillance.<sup>189</sup>

Compliance with the rule of law shifts focus towards questions such as *what* legal discretion that is granted to authorities, *how* the secret surveillance is performed and *who* is empowered with legal competence. Consequently the legal basis is to comprise provisions on the scope granted to authorities and on the manner of exercise.<sup>190</sup> The rule of law also implies that interferences of rights under protection should be subject to effective control.<sup>191</sup>

As to distinctions between the qualitative criteria, one could argue that both accessibility and foreseeability derives from the general notion of the rule of law.<sup>192</sup> It is however a prerequisite for a fruitful discussion that one accepts that the criteria in question are autonomously defined by the Court rather than exclusively derived from external sources. This thesis thus aims to elaborate on the Court's reasoning on these criteria in the field of secret surveillance. The following suggested distinctions are the point of departure for the subsequent elaboration:

- Foreseeability mainly concerns the legal basis from an *a priori* perspective rather than addressing the employment. This implies an examination of the circumstances in which secret surveillance may be triggered and to whom it may be applied. Studies regarding foreseeability generally disregard questions about detailed application by authorities.
- The rule of law criterion excludes accessibility and foreseeability aspects and primarily examines issues on the scope of discretion granted to authorities, the manner of exercise under the discretion and control mechanisms. The rule of law criterion therefore mainly concerns the basis for how authorities' powers are exercised rather than under what conditions they are exercised.

---

<sup>188</sup> Ch. 5.2.3.3.

<sup>189</sup> Ibid.

<sup>190</sup> Case of Weber and Saravia, *supra* note 89, para. 94, case of Liberty and others, *supra* note 60, para. 62, c.f. case of Malone, *supra* note 143, para. 79.

<sup>191</sup> Ch. 5.2.3.5.

The above-suggested distinctions are generally noticeable where the Court accounts for the legal situation, but might be less apparent when the merits are subsequently applied. Hence there is often no apparent correlation between a criterion as such and its impact on the legal reasoning in favour of a judgement. This thesis manages that circumstance by attempting to relate the Court's legal reasoning with the objectives identified for each criterion, in order to find the underlying source of the Court's conclusions.

### 5.2.3.2 *Executive summary of key case law*

This section summarises the key European Court cases that are elaborated in the subsequent sections. The summary address aspects originating from the legality condition in accordance with the above delimitation.<sup>193</sup>

The judgement in the case of *Liberty and others* was delivered in 2008 and concerned the British secret surveillance legislation hereafter named 'the 1985 act'. The provisions under review authorised interception of telecommunications to and from the UK for the purpose of national security, prevention of serious crime and for safeguarding the economic well-being.<sup>194</sup> The questions of law may be summarized in two parallel tracks: on one hand the process for obtaining and employing warrants for interception, and on the other hand provisions of protection to be implemented when issuing a warrant, named the 'section 6 arrangements'.<sup>195</sup> The Court held that the 1985 act constituted a violation of article 8 due to the lack of making available the 'section 6 arrangements' and by reason of not indicating the scope and manner of exercise conferred for the secret surveillance operations.<sup>196</sup>

The *Weber and Saravia* judgement was passed in 2006. The impugned national legislation, the G 10 act, had previously been the subject of assessment and amendment by the German Federal Constitutional Court.<sup>197</sup> Consequently, it was the amended version of the act that

---

<sup>192</sup> Koch Ida Elisabet & Vedsted-Hansen Jens, *International Human Rights and National Legislatures - Conflict or Balance?*, Nordic Journal of International Law, vol. 75, no. 1, 2006, p. 8.

<sup>193</sup> Ch. 5.1.

<sup>194</sup> Case of *Liberty and others*, *supra* note 60, paras 18-20.

<sup>195</sup> *Ibid.* For the former track, see *supra* note 60. The process is chronologically described by the applicants in para. 43, and the relevant domestic law and practice are described in paras 16-40. For the latter track, see para. 27. The 'section 6 arrangements' resembles the notion of minimization of surveillance, c.f. Cameron, *supra* note 40, pp. 106-7.

<sup>196</sup> *Ibid.*, para. 69.

<sup>197</sup> "G 10" refers to the act's constitutional basis in article 10 of the German Constitution.

was under review by the European Court.<sup>198</sup> The applicants alleged that the German ‘strategic monitoring’ program violated their rights pursuant to article 8. The target of the secret surveillance was primarily ether-based communications, which comprised approximately 10 per cent of the total volume of telecommunications in Germany.<sup>199</sup> Strategic monitoring was authorised for the purpose of collecting information necessary for the ‘timely identification and avoidance’ of a set of serious offences.<sup>200</sup> The complaints were held ill-founded, as the European Court concisely held that the provisions on legality were compliant with the established minimum requirements on secret surveillance.<sup>201</sup>

In 1978 the European Court reviewed an older version of the above-mentioned G 10 act in the case of *Klass and others*. The legislation empowered authorities to, inter alia, inspect mail and record telephone conversations when there were factual indications for suspecting an individual of certain serious crimes.<sup>202</sup> The applicants primarily questioned the shortage of notification following interception, which would exclude remedies before courts. The judgement mainly brought to attention the necessity of the measures in question, and the Court found no violation of article 8.<sup>203</sup>

A parallel between these legislative frameworks is the pursuit of national security. Without attempting to give substance to the notion of national security, the parallel element is the intent to protect the states from a number of serious threats.<sup>204</sup> Secret surveillance is also employed in ordinary criminal procedure legislation.<sup>205</sup> In fact a number of European Court practises originate from the sphere of criminal procedure law, such as the cases of *Malone*, *Huwig* and *Kopp*, which are further elaborated below.

---

<sup>198</sup> Case of Weber and Saravia, *supra* note 89, para. 63, and the German Federal Constitutional Court (BVerfG), 1 BvR 2226/94 of 07/14/1999, paragraphs no. (1 - 308), hereafter cited as the ‘amended G 10 act’, at [http://www.bverfg.de/entscheidungen/rs19990714\\_1bvr222694en.html](http://www.bverfg.de/entscheidungen/rs19990714_1bvr222694en.html), accessed on November 11<sup>th</sup> 2008.

<sup>199</sup> Case of Weber and Saravia, *supra* note 89, paras 26, 30 and 110. See ch. 1.1 for a technical background.

<sup>200</sup> *Infra* note 267.

<sup>201</sup> Case of Weber and Saravia, *supra* note 89, paras 96-102.

<sup>202</sup> Case of Klass and others, *supra* note 119, para. 17. N.b the different target in comparison with the general monitoring program under review in Weber and Saravia, see case of Klass and others, paras 17, 25 and 51.

<sup>203</sup> *Ibid*, para. 10, as distinct from the legitimacy of the interference caused by secret surveillance.

<sup>204</sup> For a discussion regarding the meaning of national security, see Cameron, *supra* note 40, pp. 39-73.

<sup>205</sup> In this specific context, criminal procedure law and law enforcement are treated as synonyms.

### 5.2.3.3 Accessibility

The criterion on accessibility aims to ensure that individuals have an indication of the legal regulations applicable to a given case.<sup>206</sup> Publication of the provisions in question is the natural way for states to fulfil their obligation under this criterion.<sup>207</sup> Accessibility is generally assessed from the perspective of the individual who is potentially affected by the state act.<sup>208</sup> The fact that legal aid may be necessary for interpretation does not deprive the provisions of their accessibility.<sup>209</sup>

*Liberty and others* provides an interesting illustration of the accessibility criterion. As mentioned in the case law summary above, the Secretary of State was obliged to implement so-called 'section 6 arrangements' when issuing warrants. These arrangements sought to minimize the privacy impact of the secret interception.<sup>210</sup> In response to the alleged violations the British Government argued that there were regulations concerning the process for selecting, disseminating and storing intercepted communications data according to the 'section 6 arrangements'.<sup>211</sup> However these regulations were internal and were consequently not incorporated in the 1985 act or otherwise made available to the public.<sup>212</sup>

The Government's position – that making available the 'section 6 arrangements' could damage the system and make up a security risk – did not receive judicial endorsement. By reference to the *Weber and Saravia* case, the European Court stated that it would be possible to set out clear provisions on the examination, use, storage, communication and destruction of data. The fact that a subsequent British act on interception made parts of its Code of Practice accessible was yet another reason why national security would not be comprised following publication.<sup>213</sup> The Court ultimately held that, since the 1985 act in particular did not make the procedures for obtaining and using intercepted communications data available to the public, the interference was not considered in accordance with law.<sup>214</sup> The

---

<sup>206</sup> Case of *Sunday Times*, *supra* note 91, para. 49. Note that this applies to the two initial sentences of the referred paragraph and not the remainder, which is partly obsolete in this context, c.f. *infra* note 240 and ch. 5.2.3.4

<sup>207</sup> Case of *Rotaru*, *supra* note 171, para. 54, and case of *Leander*, *infra* note 208, paras 52 and 53.

<sup>208</sup> Case of *Leander v. Sweden*, application no. 9248/81, para. 50, and case of *Kopp*, *infra* note 242, para. 55.

<sup>209</sup> *Supra* note 206.

<sup>210</sup> Case of *Liberty and others*, *supra* note 60, para. 27. The case law summary is located in chapter 5.2.3.2.

<sup>211</sup> *Ibid*, paras 48-51.

<sup>212</sup> *Ibid*, para. 66.

<sup>213</sup> *Ibid*, para. 68.

<sup>214</sup> *Ibid*, para. 69. Note the relevant passage that states: 'In particular, it did not, [...] set out in a form accessible to the public'.

emphasis on the failure to make ‘the section 6 arrangements’ available suggests that the lack of accessibility was a major contributor to the violation.<sup>215</sup>

The Court’s findings in *Liberty and others* may not have revealed the advocated distinction between qualitative criteria, in particular accessibility and foreseeability.<sup>216</sup> Rather they are discussed simultaneously without any clear distinction. This may be due to the applicant’s legal reasoning.<sup>217</sup>

Is it nevertheless viable to elaborate on the relation between the criteria based on the Court’s reasoning? As previously suggested in this thesis, accessibility may be described as a formal criterion that does not set out requirements aimed at the substantial provisions at stake. Instead it aims to ensure that provisions are made accessible so that individuals have an indication of the legal rules applicable to a given case.<sup>218</sup> That would be the opposite of the foreseeability and rule of law criteria, which impact on the substantial provisions.<sup>219</sup>

Do the above conclusions imply that the accessibility criterion is influenced by requirements originating from the other two criteria and call for their availability in the legal basis? There seem to be no indication that the accessibility assessment takes into account aspects of foreseeability or rule of law. Rather the reasoning on accessibility in *Liberty and others* addressed the fact that the impugned act provided no indication on vital parts of the provisions applicable. The alternative, to scrutinize the quality of these unavailable provisions, would have been unnecessary since the prior accessibility condition was not met.<sup>220</sup> Consequently, non-compliance with the accessibility criterion would be sufficiently established when provisions that regulate the interference are not made accessible to the individuals concerned.<sup>221</sup> As to the relation to foreseeability and rule of law, accessibility could be characterised as both an independent and a formal criterion.

---

<sup>215</sup> Ibid.

<sup>216</sup> C.f. case of Weber and Saravia, *supra* note 89, para. 92, and case of Kopp, *infra* note 242, paras 62 and 63, where the distinction is clearer.

<sup>217</sup> Case of Liberty, *supra* note 60, para. 60, which alternatively would suggest that foreseeability derives from accessibility.

<sup>218</sup> *Supra* note 206.

<sup>219</sup> Chs. 5.2.3.4 and 5.2.3.5.

<sup>220</sup> See ch. 5.2.1 regarding that the non-compliance with one condition constitutes a violation regardless of the following assessment.

<sup>221</sup> C.f. van Dijk Pieter, van Hoof Fried, van Rijn Arjen & Zwaak Leo, *Theory and Practice of the European Convention on Human Rights*, 4 edition, Intersentia, Antwerpten and Oxford, 2006, hereafter cited as van Dijk et al., pp. 336-9.

It might be possible to discern a change, over the last several decades, towards a strengthened view on accessibility in the field of secret surveillance.<sup>222</sup> In the case of *Christie*, delivered in the mid 1990's, the 1985 act was impugned on the same basis as in *Liberty and others*.<sup>223</sup> The applicant also made analogous claims on lacking accessibility and foreseeability.<sup>224</sup> The Commission in *Christie* held that accessibility with regards to the 1985 act did not reach a level of non-compliance, since the relevant provisions were set forth in the statutes.<sup>225</sup> The Commission did not touch upon the fact that while the 'section 6 arrangements' were reviewed by the Commissioner, they still remained unavailable to the individuals concerned. That in turn made it impossible for individuals to learn about the provisions applicable to the interception of communication. In fact the 'section 6 arrangements' were discussed in relation to foreseeability and were held to be compliant by virtue of the fact that the arrangements were reviewed and reported on by the Commissioner.<sup>226</sup>

In *Liberty and others* the Court differed, in holding that the 'section 6 arrangements' should be set out in a form accessible to the public.<sup>227</sup> The difference outlined between the Commission's and the Court's assessments clearly suggest that the accessibility criterion gained a stronger position in the latter judgement. It furthermore raises questions about the present Commission's legal reasoning; what made the 'section 6 arrangements' accessible when the mere legislative instruction, as distinct from substantial law, was made available to the individuals concerned?

One apparent difference is that the Court's reasoning in *Liberty and others* was distinctly coupled to the purpose of accessibility set out in the earlier case of *Sunday Times*, namely to give individuals an indication of the legal rules applicable to a given case.<sup>228</sup> In contrast, the Commission seem to have adopted an indirect interpretation of accessibility, in holding that the provisions were made available to the Commissioner.<sup>229</sup>

---

<sup>222</sup> The comparison is made between the referred cases and does not intend to comprehend the entire field of secret surveillance.

<sup>223</sup> Case of *Christie v. the United Kingdom*, application no. 21482/93. Other acts were also the subject of the Court's review.

<sup>224</sup> *Ibid*, see section B (i) on the impugned acts of 1985 and 1989. See the section named 'complaints' on the similarities with the case of *Liberty and others*, *supra* note 60.

<sup>225</sup> *Ibid*, under 'the law' and 'in accordance with law' headers.

<sup>226</sup> *Ibid*, loc. cit., c.f. *supra* note 210.

<sup>227</sup> Case of *Liberty and others*, *supra* note 60, paras 67 and 69 respectively.

<sup>228</sup> *Supra* note 206.

<sup>229</sup> *Supra* note 225.

An interesting observation is that the Court articulated the accessibility criterion in *Liberty and others* by stating that the provisions in question should be set out in a form accessible to the public.<sup>230</sup> How does that cohere with the above definition – reconfirmed in an array of cases – which states that the provisions should be accessible to the individuals concerned?<sup>231</sup>

The Court's reasoning in *Liberty and others* is arguably not indicating a change of direction. It is in fact appropriate to suggest that it is a consistent way of assessing accessibility in the field of secret surveillance. The rationale for that point of view is contemporary technological developments in the field of communication. As an illustration, data routing in the global network often depends on technical and economic drivers rather than geographical drivers.<sup>232</sup> Thus communication between individuals in one country is frequently routed via other regions. It is furthermore of relevance that the impugned British legislation, like many other secret surveillance programs, interfered with an array of communication means, such as e-mail, facsimile and telephony.<sup>233</sup> Collectively these aspects entail that the number of individuals subject to interception is extensive. Accordingly the British Government in *Liberty and others* admitted, in principle, that anyone who sent or received any form of telecommunication outside the British Islands at the time could have had their communication intercepted.<sup>234</sup> The merits of *Liberty and others* therefore suggest that the surveillance theoretically could have concerned any citizen. That condition gives an explanation to the Court's extensive interpretation of accessibility, in requiring that the provisions were to be made available to the public.

At a general level, the above conclusion entails that the magnitude of the interference has a corresponding impact on the interpretation of the accessibility criterion. A prerequisite for a well-founded assessment is therefore that the number of individuals concerned by the interference is thoroughly investigated.

---

<sup>230</sup> *Supra* note 227.

<sup>231</sup> *Supra* notes 206 and 208, see also the case of *Malone*, *supra* note 143, para. 66.

<sup>232</sup> Cf. prop. 2006/07:63, *supra* note 9, paras 69, 171, 173-4.

<sup>233</sup> Case of *Liberty and others*, *supra* note 60, paras 5, 42 and 56-7.

<sup>234</sup> *Ibid*, para. 64.

#### 5.2.3.4 Foreseeability

Is a criterion on foreseeability plausible in the field of secret surveillance? An obvious difficulty is that, by its very nature, covert measures might strike at foreseeability, since the value depends on the target's lack of awareness of the interference. This section will elaborate on the European Court's contextual interpretation of foreseeability and its impact on the national legal frameworks that enable secret surveillance.

The general notion of foreseeability is that regulations are formulated to enable individuals to regulate their conduct.<sup>235</sup> The Court has held that individuals should be able to foresee the consequences that a given action may entail, to a reasonable degree in the circumstances.<sup>236</sup> However, foreseeability is not a static concept, and it has been interpreted from a contextual standpoint by taking into account the type of measure in question.<sup>237</sup> The case of *Malone* is an important milestone in this direction, since the Court herein expressed that foreseeability cannot mean the same thing when intercepting communication for the purpose of a police investigation, as compared to when the law aims to restrict the conduct of individuals.<sup>238</sup> The notion of foreseeability is therefore somewhat more lenient for secret surveillance than in other fields of operation of article 8.<sup>239</sup>

The Court maintained its position in *Weber and Saravia*, holding that foreseeability does not imply that individuals are entitled to be aware of when authorities are likely to commence using secret surveillance, so that they can adapt accordingly.<sup>240</sup>

What level of clarity does the Convention require for the legal basis that authorises the secret surveillance? One guiding statement from the Court is that the basis should be sufficiently clear to give individuals adequate indication regarding the circumstances and conditions for when authorities may resort to secret measures.<sup>241</sup> The stringency is somewhat linked to the seriousness of the measure in question, which in the field of secret surveillance generally entails that provisions are to be *particularly* precise, especially as the

---

<sup>235</sup> Case of *Sunday Times*, *supra* note 91, para. 49, and *van Dijk et al.*, *supra* note 221, p. 337.

<sup>236</sup> *Ibid*, loc. cit.

<sup>237</sup> C.f. *ibid* and the case of *Leander*, *supra* note 208, para. 51, and the case of *Weber and Saravia*, *supra* note 89, para. 93.

<sup>238</sup> Case of *Malone*, *supra* note 143, para. 67.

<sup>239</sup> *Supra* note 237.

<sup>240</sup> Case of *Weber and Saravia*, *supra* note 89, para. 93, reiterated in the case of *Liberty and others*, *supra* note 60, para. 62. C.f. the previous and partly deviating conclusion in the case of *Sunday times*, *supra* note 91, para. 49.

technology available is continually becoming more sophisticated.<sup>242</sup> An analysis of the magnitude of the interference would thus be necessary in order to learn the level of foreseeability required for a given case.

On the contrary, the Court has declared that absolute precision is unattainable in keeping pace with changes in society.<sup>243</sup> That statement reasonably implies that regulatory frameworks *per se* comprise a space of interpretation in order to function when applied by authorities. That space is arguably corresponding with the legal differentiation between a decision and a provision.

In addition to the above general statements on foreseeability, the Court has set out a number of minimum requirements applicable to secret measures of surveillance in general.<sup>244</sup> These minimum requirements oblige the legal basis to provide for:

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 data obtained,
5. the precautions to be taken when communicating data to other parties, and
6. circumstances in which recordings may or must be erased or tapes destroyed.<sup>245</sup>

Before examining the substantial law aspects of these requirements, it would be appropriate to investigate their systematization according to the suggested structure which distinguishes between the foreseeability and rule of law criteria.<sup>246</sup> The Court seems to have developed these requirements in relation to secret measures in general, without reference to any distinction between the qualitative criteria. Given the suggested structure, it is

---

<sup>241</sup> Case of Malone, *supra* note 143, para. 67, referred in Liberty and others, *supra* note 60, para. 62, and Weber and Saravia, *supra* note 89, para. 93. C.f. case of Leander, *supra* note 208, para. 51.

<sup>242</sup> Case of Kopp v. Switzerland, application no. 13/1997/797/1000, para. 72. This judgement's applicability in terms of signals intelligence programs was confirmed in case of Liberty and others, *supra* note 60, para. 63. See also the case of Huvig, *supra* note 82, para. 32.

<sup>243</sup> Case of Olsson v. Sweden (No. 1), application no. 10465/83, para. 61(a).

<sup>244</sup> Also referred as 'safeguards', see Sottiaux Stefan, *Terrorism and the Limitation of Rights: The ECHR and the US Constitution*, Hart Publishing, Oxford and Portland, 2008.

<sup>245</sup> Weber and Saravia, *supra* note 89, para. 95, reiterated and formally extended with regards to applicability in the case of Liberty, *supra* note 60, para. 62. Also referred in the case of the Association for European Integration and Human Rights and Ekimdzhev v. Bulgaria, application no. 62540/00, para. 76.

<sup>246</sup> As set out in ch. 5.2.1., and subsequently elaborated.

reasonable that requirements one and two are tied to the foreseeability criteria, following its purpose of providing indications as to the circumstances and conditions for when authorities are empowered to secret measures.<sup>247</sup> In other words requirements one and two correspond to the question about *when* these measures can be invoked, which naturally links to foreseeability.

The remaining requirements three to six, on the other hand, reasonably articulates the rule of law criterion by relating to the inherent purpose of defining the scope of discretion and setting out the manner of exercise for the authorities which operate under the legal basis.<sup>248</sup> The procedure to be followed for examining, storing and sorting data, as well as precautions on disseminating data, are submitted to be relevant rule of law aspects in accordance with the Court's case law.<sup>249</sup> Hence these aspects will be discussed in the following section.

From a legislative perspective one should note that the minimum requirements are to be set out in *statutory* law, according to the Court.<sup>250</sup> This explicit reference to the constitutional rank of law is clearly a deviation from the requirement that interferences are to have a basis in national law, regardless of whether it is statutory, subordinate or case law.<sup>251</sup> The fact that the Court hereby stresses the rank of law to set out the minimum requirements ought to reflect the particular importance acknowledged to the field of secret surveillance.<sup>252</sup> An apparent consequence for the legislator is that measures which fall under the minimum requirements of article 8 will have to be taken into consideration during the legislative process.

A glimpse at the previously-mentioned case of *Christie* suggests that the latter explicit reference to constitutional rank reinforces requirements on foreseeability. When assessing the impugned 1985 act, the Commission held that foreseeability was upheld even though general and unlimited provisions were explained by administrative or executive statements

---

<sup>247</sup> Ch. 5.2.3.1.

<sup>248</sup> *Ibid.*

<sup>249</sup> E.g. case of Rotaru, *supra* note 171, paras 57 and 61.

<sup>250</sup> *Supra* note 245.

<sup>251</sup> C.f. ch. 5.2.2.

<sup>252</sup> C.f. the European Commission for democracy through law (Venice Commission), *Report on the democratic oversight of the security services*, Venice, 2007, p. 5, para. 13.

and instructions.<sup>253</sup> The Commission's conclusion would clearly not be tenable today due to the Court's requirements on setting out the minimum requirements in statutory law.

It has been argued in the legal doctrine that it is somewhat unclear as to the extent to which these minimum requirements apply to general surveillance programs, since they were originally developed for monitoring of individuals in the course of criminal procedure law.<sup>254</sup> In *Liberty and others* the Court held that there would be no reason for not applying the minimum requirements to general programs of monitoring, even though they were initially developed in relation to individual monitoring.<sup>255</sup> The circumstances in *Liberty and others* illustrate this expansion of scope, as the alleged monitoring facility was asserted to intercept 10,000 simultaneous external telecommunications channels.<sup>256</sup> The impugned 1985 act in *Liberty and others* provided for both individual and general monitoring, but only the latter was applicable on the merits.<sup>257</sup>

The minimum requirements had in fact been applied in *Weber and Saravia*, delivered two years earlier.<sup>258</sup> However, at that point the Court did not address the difference in monitoring scope from previous judgements.<sup>259</sup> The target of so-called strategic monitoring challenged in *Weber and Saravia* was primarily ether-based communications, which comprised approximately 10 per cent of the total volume of telecommunications in Germany.<sup>260</sup> Cable-based communications were subject to interception only for identification and prevention of an armed attack on Germany.<sup>261</sup> In sum, the present monitoring scope is evidently in contrast with individual monitoring programs previously assessed by the Court, such as in the *Klass and others* case.<sup>262</sup> Therefore there is arguably no rationale to conclude other than that the judgements of *Liberty and others* and *Weber and*

---

<sup>253</sup> Case of *Christie*, *supra* note 223, under the 'in accordance with law' header, in the paragraph commencing 'While, as the applicant points out'.

<sup>254</sup> *Sottiaux*, *supra* note 244, see also case of *Huvig*, *supra* note 82, and case of *Valenzuela Contreras v. Spain*, application no. 58/1997/842/1048, para. 46. *Sottiaux* would have reached this conclusion having available the *Weber and Saravia* judgement but not *Liberty and others*.

<sup>255</sup> Case of *Liberty and others*, *supra* note 60, para. 63. The statement would reasonably refer to the 'above requirements', namely the paras 93-5 in the case of *Weber and Saravia*.

<sup>256</sup> Case of *Liberty and others*, *supra* note 60, para. 5.

<sup>257</sup> *Ibid*, paras 22-3, 44, 64-5 and 5.

<sup>258</sup> Case of *Weber and Saravia*, *supra* note 89, para. 95.

<sup>259</sup> *Infra* note 262.

<sup>260</sup> Case of *Weber and Saravia*, *supra* note 89, paras 26, 30 and 110.

<sup>261</sup> Case of *Weber and Saravia*, *supra* note 89, paras 97 and 27, and the amended G 10 act, *supra* note 198, para. 8.

<sup>262</sup> C.f. case of *Weber and Saravia*, *supra* note 89, paras 3 and 4, and case of *Klass and others*, *supra* note 119, paras 17, 25 and 51.

*Saravia* transferred a number of safeguards, originally developed for individual monitoring programs, to monitoring programs with a considerably larger scope.

There are further distinctions of relevance from an applicability point of view. The Court applied the above minimum requirements in *Liberty and others* even though the circumstances differ from those of *Weber and Saravia* with regards to the means of communication subject to interception.<sup>263</sup> The former case concerned an array of communication means, such as e-mail, facsimile and telephony, while the latter only concerned telephony.<sup>264</sup> Since the Court applied the equivalent requirements in *Liberty and others*, it is reasonable to argue that the article 8 protection applies to all means of communication. That point of view is also consistent with the above conclusions about the scope of article 8.<sup>265</sup> As a consequence, the notion of ‘telephony’ in the minimum requirements should be read as ‘communication’.

Turning from applicability to interpretation aspects, a set of judgements passed by the Strasbourg machinery will be illustrated to elaborate the foreseeability criterion. A leading case in this field is *Weber and Saravia*, where the proceedings against the German legislation were held ill-founded.<sup>266</sup> What characteristics made the amended G 10 act compliant with the requirements on foreseeability? At the outset, strategic monitoring was permitted for the purpose of collecting information necessary for the timely identification and avoidance of a set of serious offences, such as armed attacks on Germany and the commission of international terrorist attacks in Germany. By explicitly enumerating the type of offences that could trigger secret surveillance, the amended G 10 act was held compliant with the first minimum requirement.<sup>267</sup> Moreover the category of individuals who were likely to have their communications intercepted was set out in statutory law. The primary category of target was individuals engaging in international ether-borne telephone conversations and

---

<sup>263</sup> Case of *Liberty and others*, *supra* note 60, paras 64-70, made applicable by para. 63.

<sup>264</sup> C.f. case of *Liberty and others*, *supra* note 60, paras 5, 42, 56, 57, with *Weber and Saravia*, *supra* note 89, paras 5, 6, 66, 77.

This would however be due to the merits of the latter case rather than the technical capabilities available at the German Federal Intelligence Service, see the German Federal Constitutional Court, *supra* note 198, para. 230.

<sup>265</sup> Ch. 4.1.

<sup>266</sup> For the Court’s assessment, see the case of *Weber and Saravia*, *supra* note 89, paras 76-136.

<sup>267</sup> The G 10 act article 3(1), see the case of *Weber and Saravia*, *supra* note 89, paras 96 and 26-31. C.f. *supra* note 260. See the German Federal Constitutional Court judgement, *supra* note 198, paras 209 and 244-6, on the restriction of offences from the original act and the explicit enumeration of offences that were the subjects of the Court’s assessment.

who used catchwords related to the enumerated serious offences.<sup>268</sup> The European Court accordingly found that the amended G 10 act gave an adequate indication on the conditions for when authorities could resort to secret surveillance. The legislation was therefore held foreseeable in this respect.<sup>269</sup>

French statute and case law on secret surveillance for criminal investigation was challenged in the case of *Huvig*, delivered in 1990, which has been cited in a number of following judgements.<sup>270</sup> The Court concluded that the French legal framework in question failed to set out both the offences that could give rise to secret surveillance and the categories of people liable to have their telephones tapped.<sup>271</sup> Even though the Court's concluding statements appear to shed light on rule of law deficiencies, it is reasonable that the above-referred foreseeability aspects impacted on the overall judgement. This assertion is based on the fact that the minimum requirements on foreseeability were not met, which decreased the possibility for individuals to learn the conditions and circumstances under which interception could be employed.<sup>272</sup>

---

<sup>268</sup> Case of *Weber and Saravia*, *supra* note 89, paras 97 and 26-32. There were two other targets: Foreign nationals whose communication was intercepted to avoid the offences listed, for which the 'catchword regulation' did not apply, and individuals using cable-borne telephony or mail who could have their communication intercepted when engaging in an armed attack on Germany, *ibid*. See, inter alia, the German Federal Constitutional Court judgement, *supra* note 198, paras 25-8 on search concepts.

<sup>269</sup> Case of *Weber and Saravia*, *supra* note 89, paras 101, 97 and 26-32. The same conclusion was reached in *Klass*, *supra* note 119, paras 45 and 51, which concerned individual monitoring pursuant to a previous version of the G 10 act. See also case of *Rotaru*, *supra* note 171, paras 55 and 57 for a similar conclusion on foreseeability.

<sup>270</sup> Case of *Huvig*, *supra* note 82. It has been cited in, inter alia, *Weber and Saravia*, *supra* note 89, para. 95, and case of *Liberty and others*, *supra* note 60, para. 62 (95).

<sup>271</sup> *Ibid*, paras 13 and 34-5.

<sup>272</sup> *Ibid*, loc. cit. Similar conclusions were reached in the case of *Kruslin*, *supra* note 67, para. 35.

### 5.2.3.5 *Compatibility with the rule of law*

Compatibility with the rule of law is an imperative criterion following its impact on a number of judgements passed by the European Court in the field of secret surveillance.<sup>273</sup>

What justifies the establishment of the rule of law criterion? On a general level, the principle of the rule of law is an inherent component in the Council of Europe by virtue of manifestations in the Convention and in the Statute of the Council.<sup>274</sup> By emphasizing the importance of implementing safeguards against abuse of protected rights, the Court has created a link between the principle of the rule of law and the legality condition.<sup>275</sup>

In cases concerning secret surveillance the Court has spelled out that powers exercised in secret entail evident risks of arbitrariness.<sup>276</sup> The rule of law criterion developed by the Strasbourg case law hence aims at providing legal protection in national legislation against abuse and arbitrary interferences with rights protected by the Convention.<sup>277</sup> The magnitude of the safeguards to be implemented for protection depends on a thorough assessment of the circumstances, such as the nature, scope and duration of the interference.<sup>278</sup>

It is outside the scope of this thesis to provide a comprehensive examination on the principle of the rule of law. The alignment is rather towards a discussion regarding the rule of law aspects on secret surveillance developed by the Court, which is referred to as the rule of law criterion.

What does the rule of law criterion require from the national legal basis that authorises an interference? It is submitted that the criterion is primarily be aligned towards the legal discretion granted to authorities and effective control of the mandate given. In particular, the Court has stated that it would be contrary to the rule of law if the legal discretion granted to authorities were expressed in terms of an unfettered power. Hence the legal basis

---

<sup>273</sup> E.g. case of Malone, *supra* note 143, para. 79, case of Liberty and others, *supra* note 60, paras 64-5 and 69, case of Rotaru, *supra* note 171, para. 61, and case of Kopp, *supra* note 242, para. 75. See also Dijk et al., *supra* note 221, pp. 338-9.

<sup>274</sup> CETS 1, signed at London May 5th 1949, entered into force on August 3rd 1949, Council of Europe, [www.Conventions.coe.int](http://www.Conventions.coe.int), accessed November 18th 2008, accounted for in the preamble and in article 3, and in the preamble of the Convention, *supra* note 22.

<sup>275</sup> Dijk et al., *supra* note 221, p. 337.

<sup>276</sup> Case of Malone, *supra* note 143, para. 67, reiterated in case of Liberty and others, *supra* note 60, paras 62-3.

<sup>277</sup> *Ibid.*

<sup>278</sup> Case of P.G. and J.H. v. the United Kingdom, *supra* note 157, para. 46, and case of Klass and others, *supra* note 119, para. 50. C.f. Cameron, *supra* note 40, pp. 102 and 127, and Sottiaux, *supra* note 244, pp. 277-8.

is to indicate the discretion granted to authorities and the manner of its exercise.<sup>279</sup> These provisions are to be set out in a clear and detailed manner.<sup>280</sup>

Furthermore, the rule of law criterion implies that interferences of rights under protection should be subject to effective control. The Court has held that judiciary control would be the normal procedure, at least in the last resort, as it offers the best guarantees of independence, impartiality and proper procedure.<sup>281</sup> Provisions regarding supervision of the empowered authorities are to be established by law.<sup>282</sup>

The right to effective remedy is also normally classified under the notion of the rule of law.<sup>283</sup> This thesis however is delimited to examining requirements originating from article 8, whereas the right to effective remedy is regulated in a separate article under the Convention and is hence not further discussed here.<sup>284</sup>

After having established some basic concepts of the rule of law criterion, the remainder of this section is dedicated to a survey on its practical impact. A point of departure is to discuss the set of minimum requirements that correspond to the rule of law criterion.<sup>285</sup>

These relevant minimum requirements oblige the legal basis to provide for:

3. a limit on the duration of telephone tapping,
4. the procedure to be followed for examining, using and storing data obtained,
5. the precautions to be taken when communicating data to other parties, and
6. circumstances in which recordings may or must be erased or tapes destroyed.<sup>286</sup>

---

<sup>279</sup> Case of Weber and Saravia, *supra* note 89, para. 94, and case of Liberty and others, *supra* note 60, para. 62, c.f. case of Malone, *supra* note 143, para. 79.

<sup>280</sup> *Ibid*, and case of S. and Marper v. the United Kingdom, applications nos. 30562/04 and 30566/04, para. 99.

<sup>281</sup> Case of Klass, *supra* note 119, para. 55. See also Cameron, *supra* note 40, pp. 157-61.

<sup>282</sup> Case of Rotaru, *supra* note 171, para. 59.

<sup>283</sup> C.f. Ehrenkrona Carl Henrik, *Rättssäkerhetsbegreppet och Europakonventionen*, SvJT, vol. 1, 2007, p. 39.

<sup>284</sup> The European Convention, *supra* note 22, article 13. For a discussion of the distinctions in this field, see Cameron, *supra* note 40, pp. 126-7. A prerequisite for effective remedy is often that the individual is notified of the interference. That aspect is not further discussed in this thesis.

<sup>285</sup> For suggested distinctions between the foreseeability and rule of law criteria in relation to the minimum requirements, see chs. 5.2.3.1, 5.2.3.4 and 5.2.3.5.

<sup>286</sup> *Supra* note 245 for the complete elaboration. See ch. 5.2.3.4 on the point that these requirements would apply to all means of communication.

These minimum requirements on the rule of law will be illustrated by leading cases from the European Court. The initial focus is to investigate aspects on the discretion granted in the process of obtaining and examining data originating from secret surveillance.

The *Liberty and others* examination will commence by looking at the process for obtaining and employing warrants for interception according to the 1985 act. Generally the Secretary of State issues a warrant.<sup>287</sup> A specification of a communication link from Britain to a foreign source to be intercepted should be included in the warrant. The warrant does normally not contain limitations of what data to be gathered.<sup>288</sup> The applicants held that the discretion granted by the 1985 act was taken advantage of by means of issuing extraordinarily broad warrants, such as 'all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe'.<sup>289</sup> The Government acknowledged that any person sending or receiving any form of telecommunications outside the British Islands at the time could have had their communications intercepted.<sup>290</sup> Hence the Court concluded that the legal discretion granted in the process of issuing warrants was practically unlimited.<sup>291</sup>

The second step in the procedure according to the 1985 act is to issue a certificate, which, in association with a warrant, constitutes a 'certified warrant'. The purpose of the certificate is to describe why data gathered under the warrant is to be examined.<sup>292</sup> The 1985 act required the Secretary of State to issue a certificate and it was sufficient to refer to one of the following grounds as a description: in the interest of national security, for the purpose of preventing or detecting serious crime,<sup>293</sup> or for the purpose of safeguarding the economic well-being of the United Kingdom.<sup>294</sup> The Court held that the impugned legislation conferred a wide discretion with regards to the data that could be obtained by a certificate.<sup>295</sup>

---

<sup>287</sup> Case of Liberty and others, *supra* note 60, paras 25 and 23.

<sup>288</sup> C.f. *ibid*, paras 64, 23 and 43.

<sup>289</sup> *Ibid*, para. 43.

<sup>290</sup> *Ibid*, para. 47.

<sup>291</sup> *Ibid*, para. 64. See also ch. 5.2.3.3.

<sup>292</sup> *Ibid*, paras 24, 26 (18), c.f. 43 and 65.

<sup>293</sup> *Ibid*, para. 19.

<sup>294</sup> *Supra* note 292.

<sup>295</sup> Case of Liberty and others, *supra* note 60, para. 65.

The subsequent steps in the procedure are the selection of data for examination, the employment of data, dissemination and deletion of the data.<sup>296</sup> The 1985 act did not account for these operations, other than the 'section 6 arrangements', which were not made available to the public and hence violated the legality condition.<sup>297</sup>

Did the rule of law criterion, as interpreted in this thesis, have an impact on the violation found in *Liberty and others*? The fact that the accessibility criterion was not complied with somewhat blurred the impact if the criteria further down in the chain of the legitimacy assessment.<sup>298</sup> Nevertheless, the Court's conclusions on the extremely broad discretion granted in the process of obtaining, examining and deleting intercepted data are all aspects falling under the notion of the rule of law; directly, as being assigned to the minimum requirement set out, and indirectly, by referring to the criterion's overarching objective that legislation should clearly indicate the scope of discretion conferred and the manner of exercise.<sup>299</sup>

These aspects were furthermore accounted for in the Court's concluding reasoning, which suggests that rule of law aspects had an actual impact on the outcome.<sup>300</sup> As previously suggested however, it is likely that the lack of accessibility was the main component of violation rather than non-compliance with the rule of law criterion.<sup>301</sup>

In contrast to *Liberty and others*, the Court's assessment in *Malone* was more clearly linked to rule of law aspects.<sup>302</sup> The legislation on interception of telephony was not contained within one legislative unit, but rather as a mixture of statutes and case law. The Court held that the legal situation was obscure and open to different interpretations. Primarily, it was not possible to distinguish between the discretion that was granted by means of the legal basis and the discretion held by the authorities themselves. As a result, the legislation did not

---

<sup>296</sup> Ibid, paras 48-52, c.f. para. 43.

<sup>297</sup> For details on what the 'section 6 arrangements' comprised, see *ibid*, paras 66, 27 and 48-52. See ch. 5.2.3.3 on accessibility aspects. The fact that provisions that would account for a number of the 'minimum requirements' were not made accessible reasonably excludes subsequent assessments on the impact on compliance with the rule of law requirement, due to the order in which the qualitative criteria are assessed, see ch. 5.1.

<sup>298</sup> Ch. 5.2.1.

<sup>299</sup> Case of *Liberty and others*, *supra* note 60, paras 62(94), 64, 65. Minimum requirements four to six would be of highest relevance for the notion of the rule of law in this context, particularly requirement number four.

<sup>300</sup> *Ibid*, para. 69.

<sup>301</sup> *Ibid*, loc. cit., c.f. ch. 5.2.3.3.

<sup>302</sup> The case of *Malone*, *supra* note 143.

comply with one of the requirements of the rule of law criterion as interpreted by this thesis, namely to indicate the scope and manner of exercise for the discretion granted to authorities.<sup>303</sup>

As discussed earlier, the allegations of violations in *Weber and Saravia* were held to be ill-founded.<sup>304</sup> The below exposition endeavours to examine the characteristics of the amended G 10 act which led the Court to find it in compliance with the rule of law criterion. An important source in this discussion is the earlier-discussed Federal Constitutional Court's assessment and amendment of the G 10 act.<sup>305</sup>

The assessment performed by the European Court essentially followed the sequence of the enumerated minimum requirements.<sup>306</sup> Accordingly, the first topic to review was aspects concerning the duration of interception. The maximum duration of monitoring was three months, with the possibility of prolonging the duration for no more than three months at a time, as long as the statutory provisions were met.<sup>307</sup> In essence the European Court held that the present provision was compliant with the minimum requirements.<sup>308</sup>

The G 10 act regulated the permitted use of information by obliging the Federal Intelligence Service to verify whether personal data<sup>309</sup> gathered was required for the objectives that justified the measure.<sup>310</sup> The provision thereby established a correlation between the serious offences for which the timely identification and avoidance strategic monitoring could be ordered, and the subsequent outcome of that monitoring. The Federal Constitutional Court found that the safeguards for unauthorised use were too weak and that the provisions failed to meet the Constitutional requirement for identification. Therefore the current provision

---

<sup>303</sup> *Ibid.*, paras 37-56 and 69-79.

<sup>304</sup> Ch. 5.2.3.4.

<sup>305</sup> The German Federal Constitutional Court judgement, *supra* note 198, and the case of *Weber and Saravia*, *supra* note 89, para. 63.

<sup>306</sup> Case of *Weber and Saravia*, *supra* note 89, paras 98-101, on the rule of law criterion. See the full amended G 10 act for a more thorough exposition on the national legal basis, *supra* note 198. See Cameron, *supra* note 40, pp. 127-31 for a discussion of the German supervision system.

<sup>307</sup> Case of *Weber and Saravia*, *supra* note 89, para. 20. These provisions are found in section 5 of the G 10 act. The requirement on setting out a limit on duration is read as 'communication' rather than telephony according to the conclusions in the present section. The provision on duration was not part of the revised G 10 act that enabled strategic monitoring, nor was it part of the amendment delivered by the Federal Constitutional Court, see *ibid.*, *loc. cit.*, and the German Federal Constitutional Court judgement, *supra* note 198.

<sup>308</sup> *Weber and Saravia*, *supra* note 89, paras 99 and 101.

<sup>309</sup> C.f. Bignami, *supra* note 34, p. 620, and Waldo, *supra* note 2, pp. 366-71.

<sup>310</sup> Section 3(4) of the G 10 act, see *Weber and Saravia*, *supra* note 89, para. 22 and *supra* notes 267 and 311.

was to be applied with the limitation that the personal data was marked and that it was *used* only for the purposes that justified its collection in the first place.<sup>311</sup>

The G 10 act contained two provisions concerning transmission of intercepted data from the German Federal Intelligence Service; namely transmission to the Federal Government and transmission to a set of other authorities, *inter alia*, the public prosecutor, police services, customs and the military counter-intelligence offices.<sup>312</sup>

In regards to transmission of data to the Federal Government, the G 10 act prior to amendment contained provisions obliging the Federal Intelligence Service to inform the Government about findings obtained by strategic monitoring, including personal data.<sup>313</sup> The Federal Constitutional Court however held that the legislation did not contain safeguards to prevent data being reported for purposes other than the original purposes, nor did it contain safeguards to ensure that the Government would not keep and use data for other purposes. Furthermore there were no identification requirements to enable traceability. Hence the Federal Constitutional Court amended the G 10 act so that the provision on transmission to the Government was to be applied with the limitation that personal data reported to the Government was marked and remained bound to the purposes which had justified the original collection.<sup>314</sup>

The second type of transfer featured in the G 10 act was transmission to other authorities.<sup>315</sup> The G 10 act permitted transmission of personal data to other authorities to a larger extent than what was permitted for the collection at the outset.<sup>316</sup> It is submitted that this entails that while only certain serious offences would justify the interference of the secret surveillance, received data that concerned an array of less serious offences could be transferred to these other authorities for prevention, resolution or persecution.<sup>317</sup>

---

<sup>311</sup> Weber and Saravia, *supra* note 89, para. 23, and the German Federal Constitutional Court judgement, *supra* note 198, paras 306 and 247-250. The purposes in this case are those listed in section 3(1). Section 3(3) will not be accounted for individually as it should be read in conjunction with section 3(5); see the Federal Constitutional Court judgement, paras 249 and 307.

<sup>312</sup> For a complete list of the latter, see the case of Weber and Saravia, *infra* note 89, para. 36. These cases are hereafter cited as 'the other authorities', reflecting the wording in the European Court's judgement.

<sup>313</sup> The G 10 act section 3(3), see the case of Weber and Saravia, *supra* note 89, para. 34.

<sup>314</sup> *Ibid*, para. 35 and the German Federal Constitutional Court judgement, *supra* note 198, paras 306 and 251-56.

<sup>315</sup> *Supra* note 312, and case of Weber and Saravia, *supra* note 89, paras 36-44.

<sup>316</sup> The German Federal Constitutional Court judgement, *supra* note 198, para. 274. The full legal reasoning on this matter is located in paras 257-81.

<sup>317</sup> *Ibid*, para. 274 and Weber and Saravia, *infra* note 89, para. 33

The Federal Constitutional Court held that the current provisions produced an imbalance to the detriment of fundamental rights.<sup>318</sup> Accordingly, the Federal Constitutional Court stated that the regulations on transfer of data to the other authorities would be applied under the condition that specific facts formed the basis of suspicion that an individual is planning, is committing or has committed one of the offences.<sup>319</sup> Offences in this context arguably include the list of less serious offences, despite the fact that the secret surveillance could only be authorised for the prevention of the previously-mentioned six serious offences.<sup>320</sup> A further condition for applying the provision on transmission was that a record of the transfer was kept.<sup>321</sup>

How did the European Court assess the amended G 10 act with regards to the above rule of law aspects, specifically the regulation on examining and using the data obtained by means of strategic surveillance? The European Court concluded concisely that the procedures for examining and using data obtained were set out in detail. Furthermore the Court confirmed that the limits and precautions on transmission laid down were further strengthened by the Federal Constitutional Court.<sup>322</sup>

Another rule of law aspect under review was the deletion of data, of which some general aspects will be discussed here. The amended G 10 act set out that if data was no longer necessary in relation to the original purpose that justified its collection, and if it was not to be transmitted to another authority, it was to be deleted by the Federal Intelligence Service. Deletion was to be recorded in minutes and supervised by a staff member qualified to hold

---

<sup>318</sup> Ibid, para. 278. The reasons would primarily be that factual indications and the mere planning of an offence would be enough for a transmission and that transfers would be permitted for less serious offences than those justifying the initial collection.

<sup>319</sup> Ibid, paras 307 and 47, cf. case of Weber and Saravia, *infra* note 89, para. 44.

<sup>320</sup> *Supra* note 317, cf. *supra* note 267. With regards to offences already committed, the Federal Constitutional Court held that transfer should be permitted to the other authorities when there was a factual basis for suspecting that an individual had committed an offence, which would correspond with the German Code of Criminal procedure. The rationale for this statement is arguably that the purpose of the G 10 act is the *timely recognition* of crimes, rather than the prosecution of already committed crimes, see section 3(1). In respect of committed crimes, this approach confirms the established criminal law framework on prosecution rather than to create a parallel system with a lowered threshold. However, this interpretation did not seem to impact on the Federal Court's concluding temporary statement, which reads '[if someone] plans, is committing or has committed', see the German Federal Constitutional Court judgement, *supra* note 198, paras 277-281, 307 and 47, cf. case of Weber and Saravia, *supra* note 89, para. 44. Hence the judgement appears to sanction transmission of personal data regarding less serious offences.

<sup>321</sup> *Supra* note 319.

<sup>322</sup> Case of Weber and Saravia, *supra* note 89, para. 99. The transfer of personal data was also reviewed under the necessity assessment.

judicial office. In order not to cause complications for judicial review, the data was required to be maintained for six months after notifying the person concerned. During this time the data in question would be sealed, in the sense that it could only be used for judicial examination.<sup>323</sup>

In addition, the authorities receiving data from the Federal Intelligence Service were required to evaluate the necessity of data obtained pursuant to the amended G 10 act. These evaluations are however submitted to differ from the evaluation undertaken by the Federal Intelligence Service. The reason for this difference is that data received by other authorities would reach the level of necessity when serving the purposes of prevention, investigation and prosecution of the *extended* catalogue of offences, as distinct from the limited set of serious offences that justified the initial collection.<sup>324</sup> Unnecessary data was to be deleted while stored data had to be marked as originating from strategic monitoring.<sup>325</sup> The six-month storage requirement for judicial review was to apply to other receiving authorities also.<sup>326</sup>

Personal data no longer necessary for the respective purposes of the amended G 10 act was required to be deleted, and a compulsory review was to take place every six months.<sup>327</sup>

There seemed to be no specific statements from the European Court on data deletion aspects, other than an enumeration of the relevant provisions pursuant to the amended G 10 act. It is necessary instead to refer back to the European Court's concluding statement that the amended G 10 act contained the minimum safeguards against abuse and arbitrary interferences, and as a result complied with the rule of law criterion.<sup>328</sup>

The final rule of law aspect to be discussed from *Weber and Saravia* is supervision of strategic monitoring operations. The amended G 10 act provided the G 10 Commission with the authority to decide on the permissibility and necessity of strategic monitoring. The Federal

---

<sup>323</sup> The G 10 act section 3(6), see the case of *Weber and Saravia*, *supra* note 89, para. 46, and the German Federal Constitutional Court judgement, *supra* note 198, paras 308, 301, 248 and 298-301. On notification, see *supra* note 284.

<sup>324</sup> The G 10 act section 3(7), see the case of *Weber and Saravia*, *supra* note 89, paras 47-50, and the German Federal Constitutional Court judgement, *supra* note 198, paras 308 and 282-85. This would correspond to the prerequisites for transmitting data to other authorities, see *supra* note 320. The basis for the transmission would be article 3(5) of the G 10 act.

<sup>325</sup> *Ibid*, loc. cit.

<sup>326</sup> *Supra* note 323.

<sup>327</sup> Case of *Weber and Saravia*, *supra* note 89, para. 48.

Minister was to obtain permission for monitoring measures and additionally inform the Commission on a monthly basis concerning planned activities. After recognizing that the Commission's authority did not sufficiently cover the entire process of screening and utilization, the Federal Constitutional Court extended the supervisory scope to cover additional parts of the operation process including, inter alia, the above-mentioned aspects on transmission of personal data to the Federal Government and to the other authorities. The second supervisory function was the G 10 Board – a body comprising nine members of parliament to perform a general review of compliance with the G 10 act every six months.<sup>329</sup>

Recalling the European Court's statement that supervision normally should be assured by the judiciary, it is apparent that the G 10 act does not conform in this regard.<sup>330</sup> This deviation can be traced back to the case of *Klass*, which concerned the very same G 10 act, however in a previous version. The Court in *Klass* acknowledged the independence of the supervisory bodies in relation to the authorities carrying out the monitoring, and furthermore the possibility of these authorities ruling objectively. The nature of the supervision in combination with supplementary safeguards provided for a sufficient balance, according to the European Court, notwithstanding the exclusion of judicial review.<sup>331</sup> The Court's reasoning in *Weber and Saravia* was largely based on the integrity of the two independent supervisory bodies, and the lack of rationale to deviate from the conclusions previously reached in *Klass* on similar supervision arrangements.<sup>332</sup>

Some comments should be made about supervisory aspects and the Court's conclusions in relation to them. In *Weber and Saravia*, the provisions on supervision were discussed under the necessity condition rather than legality.<sup>333</sup> As previously concluded, characteristics of the legal basis may be relevant to different parts of the legitimacy assessment, and supervisory aspects would be no exception to this.<sup>334</sup> Practically, that reasonably implies that the supervision of secret surveillance operations may be assessed under both the

---

<sup>328</sup> Ibid, paras 100-101.

<sup>329</sup> The G 10 act section 9, see the German Federal Constitutional Court judgement, *supra* note 198, paras 42-44 and 302-4 and *Weber and Saravia*, *supra* note 89, paras 24-5 and 55-8. See also Cameron Iain, *European Court of Human Rights: April 2006 – March 2007*, European Public Law, vol. 13, no. 4, 2007, pp. 547-51.

<sup>330</sup> *Supra* notes 281 and 282. Note that supervision is discussed under the necessity assessment if the former case and under legality in the latter case; see the below discussion in this section.

<sup>331</sup> Case of *Klass*, *supra* note 119, para. 56.

<sup>332</sup> Case of *Weber and Saravia*, *supra* note 89, para. 117.

<sup>333</sup> *Infra* note 336. Cf. Sottiaux, *supra* note 244, p. 289.

<sup>334</sup> C.f. ch. 5.1, Cameron, *supra* note 40, pp. 103 and 126, and case of *Klass and others*, *supra* note 119, para. 50.

legality and necessity conditions. As to the former, this thesis suggests that supervision derives primarily from the rule of law criterion and thus impacts on the legislative framework that authorises secret surveillance.<sup>335</sup> Supervision aspects may also be taken into account in the necessity assessment, when balancing national security interests of states in relation to interferences with individuals' rights to privacy.<sup>336</sup> However, it is reasonable to conclude that the Court did not consider the supervisory aspects in *Weber and Saravia* to reach a sufficient level of relevance under the legitimacy assessment, unlike the conclusions made in, for example, *Rotaru*.<sup>337</sup> This is assumed to explain why similar questions of law may arise under different conditions of legitimacy.

What conclusion may be drawn from the European Court's reasoning in the above cases? It is arguable that there is no general and absolute requirement of judicial control in the field of secret surveillance.<sup>338</sup> Rather, each qualitative criterion is somewhat dynamic, in the sense that the magnitude of the interference – such as the nature, scope and duration – has a corresponding impact on the interpretation of the criterion.<sup>339</sup>

However, following the spirit of the *Klass* reasoning, partly affirmed in *Weber and Saravia*, judicial control would be the normal procedure. The Court nonetheless found that it was within the limits of necessity to exclude judicial control, since the supervisory bodies featured in the G 10 act would provide for sufficient independency to give an objective ruling.<sup>340</sup> Again, this assessment was performed as part of the necessity assessment; hence this is why the necessity criterion was the benchmark. Conversely, the lack of supervision in *Rotaru* was held to be non-compliant with the legality condition, since the Romanian legislative framework did not provide an acceptable level of protection as required by the rule of law criterion.<sup>341</sup>

To sum up, the above discussion has confirmed that supervisory aspect may fall under both the legality and the necessity conditions. Of primary interest in this thesis are the

---

<sup>335</sup> E.g. case of *Rotaru*, *supra* note 171, paras 59-60.

<sup>336</sup> Case of *Weber and Saravia*, *supra* note 89, paras 106-7.

<sup>337</sup> C.f. *supra* notes 336 and 335.

<sup>338</sup> This conclusion does not concern aspects on effective remedy, see *supra* note 284.

<sup>339</sup> See the discussions for each qualitative criterion in chs. 5.2.3.3, 5.2.3.4 and 5.2.3.5, and *supra* note 278 for the rule of law criterion.

<sup>340</sup> Case of *Weber and Saravia*, *supra* note 89, para. 56. C.f. the case of the Association for European Integration and Human Rights and *Ekimdzhev v. Bulgaria*, *supra* note 245, for additional relevant aspects of the supervision.

requirements originating from the legality condition and specifically the rule of law criterion, as it requires that interferences of protected rights should be subject of effective control.<sup>342</sup> The European Court's legal reasoning implies that there is no general or absolute requirement on judiciary supervision in the field of secret surveillance. This thesis rather suggests that the Court's requirements on supervision ultimately depend on the nature of the interference in relation to the objective of the legitimacy condition at issue.

---

<sup>341</sup> *Supra* note 335.

<sup>342</sup> *Supra* note 281.

## 6 Concluding remarks on the legality condition

This final chapter takes a broader perspective, and concludes the thesis by discussing a handful of selected subjects originating from the legality condition.

### 6.1 Summary of conclusions on legality

The discussion in the previous chapter illustrates the European Convention requirements on legality that apply to secret surveillance legislation. The legality condition is one of the three components constituting the legitimacy scheme.<sup>343</sup> This thesis suggests the legality condition is described as a dual object.<sup>344</sup> On one hand, it requires that there is a legal basis for the privacy interference. On the other, the legality condition encapsulates three qualitative criteria that apply to legislative frameworks authorising secret surveillance.<sup>345</sup>

The qualitative criteria are arguably the essential part of the legality condition, due to the potential impact on the national legislation. Firstly, the accessibility criterion requires that individuals have an indication of the provisions that authorise secret surveillance. The second qualitative criterion requires a degree of foreseeability, so that individuals have an adequate indication of the circumstances and conditions of when authorities may resort to secret measures. Finally, the rule of law criterion requires that the legislation indicate the discretion granted to authorities and the manner of exercise. The rule of law criterion furthermore implies that the interference of rights should be subject to effective control.<sup>346</sup>

The exposition has demonstrated that the qualitative criteria are relatively dynamic, in the sense that the magnitude of interference has a corresponding effect on the level of protection required. To illustrate, the accessibility criterion appears to have been reinforced correlative to the broadened target of secret surveillance. Additionally, the level of protection required by the rule of law criterion will depend on, inter alia, the number of individuals concerned, the nature of the interference and the duration of the interference.<sup>347</sup>

---

<sup>343</sup> Chs. 3.2.2.2 and 5.1.

<sup>344</sup> Ch. 5.2.1.

<sup>345</sup> Ch. 5.2.3.

<sup>346</sup> Chs. 5.2.3.3 to 5.2.3.5.

## 6.2 Suggested model for application

Following the identification and analysis of an array of European Convention requirements, it is appropriate to look more closely at the application of the above findings. Accordingly, a suggested model to visualise the elements of the legality assessment is elaborated below. Rather than departing from a qualitative criterion point of view, the aim is to describe the requirements from a layered perspective. The substance of the model is based on this thesis's interpretation of the legality condition. Hence, the intention is neither to cover other aspects of the Convention, nor to account for the Court's general interpretive methods.<sup>348</sup> It is presupposed that an interference is recognized and that it has a basis in national law.<sup>349</sup>

This model assumes that the requirements on legality in the field of secret surveillance can be articulated by means of three layers, namely:

1. The *minimum layer*, which represents the qualitative criteria by means of the well established minimum requirements.
2. The *application layer*, which expresses the Court's interpretation and application of the qualitative criteria through its case law.
3. The *foundation layer*, which expresses the Court's underlying objectives of the qualitative criteria by statements on the criteria's intended achievement.

By way of reiteration, the qualitative criteria derives from the Conventions' 'quality of law' requirement, and necessitates that the legal basis which authorises an interference is accessible, foreseeable and in compliance with the rule of law.<sup>350</sup>

How would the model be employed? The legality assessment should commence with a review of the legislative framework in question in relation to the *minimum layer*. This layer is assumed to render factual characteristics to be assessed against the legislative framework in question. The reason for starting the assessment at the minimum layer is that its requirements are relatively practical and do not involve complex interpretations.

---

<sup>347</sup> Ibid.

<sup>348</sup> Cf. Cameron, *supra* note 56, pp. 71-3.

<sup>349</sup> Ch. 5.2.2.

<sup>350</sup> Ch. 5.2

As the minimum requirements are relatively fixed, they will not provide guidance on issues outside their explicit area. The *application layer*, on the other hand, provides for a relatively flexible approach; it represents the Court's interpretations of a qualitative criterion in a given case. The consequent assessment of a legislative framework's compliance would primarily be focused on finding similar elements in the Court's case law. It is evident that the room for interpretation would be expanded in relation to the minimum layer.

The suggested model for assessment would not be satisfactory if it did not provide recourse to issues not previously accounted for. The *foundation layer* enables assessments of aspects which would fall outside the minimum or application layers. The essence of the foundation layer is the objective of each qualitative criterion as elaborated by the Court. Subsequently, the assessment is performed by considering whether the legislative framework in question complies with the objective of a given qualitative criterion. This would be an additional step of interpretation, in comparison with the application layer.

The dynamics of the legality condition entail that each model layer ought to be taken into account in the legality assessment. The minimum layer constitutes the lowest acceptable level of protection, and features relatively legible requirements. The magnitude of the interference may however concern aspects of the application and foundations layers, and thereby necessitate higher or additional levels of legality.

### **6.3 The rationale for lenient foreseeability**

The earlier discussion on foreseeability identified that the Court has employed a context-based interpretation of foreseeability.<sup>351</sup> This practice, established in early case law, was herein labelled 'lenient foreseeability', as it lowered the general level of foreseeability established. It is evident that the Court appears to have retained this lenient foreseeability in descendant cases, notwithstanding substantially different merits. As an illustration, the case of *Malone* concerned interception in criminal procedure law, whereas *Weber and Saravia* and *Liberty and others* featured interception without prior suspicion in the pursuit of national

---

<sup>351</sup> Ch. 5.2.3.4.

security.<sup>352</sup> Irrespective of the differences, the lenient foreseeability was applied in the latter judgements.

The rationale for this remark is that the motive for deviating from the general notion of foreseeability in *Malone* would have been the ‘special context of interception of communications for the purposes of police investigations [...]’.<sup>353</sup> In the subsequent national security case of *Klass and others*, the Court addressed the prevailing requirement on prior suspicion pursuant to the G 10 act.<sup>354</sup> Once again, reviewing the G 10 act approximately 30 years later, in *Weber and Saravia*, the Court reapplied lenient foreseeability. The fact that the amended G 10 act at this point no longer required prior suspicion for secret surveillance was not the subject of any legal discourse in the Court’s elaboration regarding foreseeability.<sup>355</sup>

It is axiomatic that secret surveillance presupposes and depends upon the target’s unawareness of the measure. On the other hand, one may argue that the extension of lenient foreseeability created an imbalance to the detriment of individuals subject to general monitoring programs, such as the German ‘strategic monitoring’.<sup>356</sup> The reason is that the absence of prior suspicion – being a requisite at the outset – is no longer affirmed in Court practice, and is furthermore not compensated by corresponding reinforcements in the legitimacy scheme.

The suggested imbalance may be illustrated by the legality condition’s dynamic nature, where aspects such as the nature, scope and duration of the interference will have a corresponding impact on the level of protection required by the qualitative criteria.<sup>357</sup> What

---

<sup>352</sup> For the case of *Weber and Saravia*, *supra* note 89, paras 9, 26-31 and 39, and the case of *Liberty and others*, *supra* note 60, paras 18-26. See ch. 5.2.3.5 regarding the requirement on ‘specific facts’ for transferring data from the Intelligence Service to a set of other authorities such as the public prosecutor and the police. However this would not be an *à priori* requirement. For a discussion regarding the notion of national security, see *Cameron*, *supra* note 40, pp. 39-73.

<sup>353</sup> Case of *Malone*, *supra* note 143, para. 67.

<sup>354</sup> *Supra* note 202, with regards to ‘factual indications’ for suspicion.

<sup>355</sup> The case of *Weber and Saravia*, *supra* note 89, paras 9, 26-31 and 39. The subject was discussed in the necessity assessment but not in relation to foreseeability, see paras 123-9. The remark would be even more accurate by virtue of the fact that the number of individuals concerned increased dramatically between the two cases, see ch. 5.2.3.4 and *infra* note 202.

<sup>356</sup> Ch. 5.2.3.2. The European Court uses the term ‘general programmes of surveillance’, see the case of *Liberty and others*, *supra* note 60, para. 63.

<sup>357</sup> The conclusion in its entirety is suggested in chs. 6.1 and 6.2, and the individual components of the legality scheme and their dynamic nature are discussed in chs. 5.2.3.3, 5.2.3.4 and 5.2.3.5.

would be the characteristics of national security and criminal procedure laws to be taken into account when assessing the level of interference they generally generate?

Firstly, the number of individuals subject to interception is evidently much greater in general surveillance programs than in individual monitoring pursuant to criminal procedure law. For instance, the surveillance program under review in the case of *Liberty and others* was capable of interfering with virtually any British citizen using telecommunications services.<sup>358</sup> Another relevant feature is that national security surveillance targeting the global network typically interferes with communication in its entirety.<sup>359</sup> That stands in contrast to the criminal procedure legislation assessed in *Malone and Kopp*, which mainly concerned telephony.<sup>360</sup>

Finally, to what extent do the purposes in question impact upon the magnitude of the interference? To begin with, it is important to distinguish between collecting intelligence and evidence, since the latter is more intrusive from a privacy perspective due to its potential impacts.<sup>361</sup> Even though there has, in the past, been a corresponding dividing line between intelligence services and law enforcement agencies, this dividing line would not be present today.<sup>362</sup> On a European Convention level, the merging between these functions can be illustrated by the case of *Weber and Saravia*. The judgement addressed the transfer of personal data from the Intelligence Service to, inter alia, public prosecutors and police services. While only a handful of serious threats to the nation of Germany justified secret surveillance at the outset, transmission of personal data for the institution of criminal proceedings was arguably permitted for a more extensive set of offences.<sup>363</sup> From an interference point of view, this merger of intelligence and law enforcement operations demonstrates that national security surveillance may ultimately encroach on privacy akin to criminal procedure surveillance. The three aspects compared hence suggest that the magnitude of national security interference is not necessarily lower than interference for the purpose of criminal procedure.<sup>364</sup>

---

<sup>358</sup> Ch. 5.2.3.3.

<sup>359</sup> Chs. 1.1, 4.2 and 5.2.3.4.

<sup>360</sup> The case of *Malone*, *supra* note 143, para. 64, and case of *Kopp*, *supra* note 242, paras 44 and 50.

<sup>361</sup> Bignami, *supra* note 34, pp. 620-1.

<sup>362</sup> Cameron, *supra* note 40, pp. 88-91, Whitfield Diffie & Susan Eva Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, second edition, MIT Press, Cambridge, Massachusetts, 2007, pp. 137-40, and Waldo, *supra* note 2, pp. 251-99.

<sup>363</sup> Ch. 5.2.3.5.

<sup>364</sup> C.f. SOU 2007:22, *supra* note 4, pp. 477-9 and *passim*.

Apart from the suggested imbalance, are there any alternatives to contemporary practice? If one acknowledges the necessity of lenient foreseeability in national security surveillance and the imbalance it produces, the challenge is to seek the Convention's inherent purpose of balancing the individual's exercise of protected rights and the state's obligation to safeguard democratic society.<sup>365</sup> From a legality perspective, there are three qualitative criteria that may be strengthened to achieve this balance.<sup>366</sup>

As more states are adopting wide-ranging surveillance programs that theoretically gain access to all citizens' communications, the area that is assumed to primarily benefit from the compensating reinforcement is the regulation of secret surveillance operations and in particular its supervision.<sup>367</sup> According to the submitted definitions above, these aspects are arranged under the notion of the rule of law.<sup>368</sup> The rationale for this conclusion is that powers exercised in secret entails a particular risk of arbitrariness, which arguably is further relevant as the amount of data available dramatically expands.<sup>369</sup>

#### 6.4 Technology – threat or possibility?

Papers that concern the interplay between privacy and technology tend to picture technology simply as a threat. Such view may conceal that technology itself is neutral and that its employment is ultimately in the hands of political will. An unbalanced view may further overshadow that technology can in fact be a way to promote privacy.<sup>370</sup> As modern society largely depends upon technological infrastructure, the question is not *if* but rather *how* to make the best use of technology.<sup>371</sup>

The European Convention was drafted nearly 60 years ago, when surveillance and communications capabilities were considerably different than today.<sup>372</sup> Notwithstanding the Convention's age, the Court appears to have acknowledged the impact of technological

---

<sup>365</sup> *Supra* note 58.

<sup>366</sup> Ch. 5.2.

<sup>367</sup> *Supra* note 12, and chs. 5.2.3.2 and 5.2.3.3.

<sup>368</sup> Ch. 5.2.3.1.

<sup>369</sup> Cf. case of Weber and Saravia, *supra* note 89, para. 93.

<sup>370</sup> Waldo, *supra* note 2, p. 119-21.

<sup>371</sup> Regarding technological dependencies see SOU 2004:32, *supra* note 13, *passim*.

<sup>372</sup> Danelius, *supra* note 42, p. 17 and ch. 1.1.

developments on privacy.<sup>373</sup> The dynamic interpretations have, in general, provided a strong framework for privacy protection with technological transparency.<sup>374</sup>

The future role of the Convention as a human rights privacy instrument is arguably dependent upon how the Strasbourg machinery manages upcoming advances in the realm of privacy and technology. Promisingly in this respect, the Court has declared that ‘it is of crucial importance that the Convention is interpreted and applied in a manner which renders its rights practical and effective, not theoretical and illusory’.<sup>375</sup>

This thesis has highlighted one area in which the contemporary employment of technology may call for the next step in the development of the Court’s privacy practice, namely the level of interference caused by intercepting incidents of communications.<sup>376</sup> The account has illustrated the emerging change in the notion of incidents, by exploring the early case of *Malone* in relation to the SIA legislative framework. The comparative analysis has suggested that the traditional separation between contents and incidents is becoming obsolete, as incidents, as contemporarily employed, may comprise a number of content-related elements. This is especially so, since the SIA targets the global network that comprises communication in its entirety. The information disclosed by incidents is furthermore highly correlated with the degree of interference caused, since incidents provide a context to contents. For instance, a fragment of contents would be less valuable without access to incidents data, such as the parties, the location and the means of communication used. These aspects collectively suggest that both contents and incidents may encroach upon privacy, and that the notions have begun to merge together as a result of technological progress.<sup>377</sup>

At this point in time, the European Court’s case law still displays a relatively clear distinction between incidents and contents.<sup>378</sup> In order to ensure that the Convention maintain its position as a dynamic framework of privacy protection, the Court should arguably acknowledge the technological development and confirm that the contemporary

---

<sup>373</sup> E.g. *supra* note 242, see also *supra* note 149 on the Court’s view on development.

<sup>374</sup> De Hert, *supra* note 41, pp. 73-4.

<sup>375</sup> The case of *Christine Goodwin v. the United Kingdom*, *supra* note 149, para. 74.

<sup>376</sup> Ch. 4.3. For definitions of incidents and contents, see ch. 2.2.

<sup>377</sup> *Ibid.*

<sup>378</sup> Ch. 4.3.

employment of incidents may reach a degree of interference equivalent to contents. Such a development would not only constitute an important landmark in the future of privacy protection, it might also influence other contemporary legal issues, such as the legality of data retention.<sup>379</sup>

The rapidly changing technological era makes it inappropriate to create technical dependencies upon which privacy protection relies. Rather, the approach to assess interferences in relation to the general notions of private life and correspondence is assumed to be a sustainable way to promote privacy.

## 6.5 Developments and a glimpse to the future

This final section seeks to identify some developments in the previously discussed case law. The thesis concludes with a glimpse to the future.

The above analysis on the legality condition has illustrated developments in at least two directions.<sup>380</sup> From a substantial requirements perspective, an evident case is the growth of minimum requirements, which were not present at the time of the early cases of *Klass and others* and *Malone*. This thesis has suggested that the collected case law supports the recognition of qualitative criterion objectives. These objectives have generally been followed by Court statements that embody the practical application of the criteria. It is submitted, as an example, that the Court has developed the rule of law criterion with the objective that national legislation is to provide protection against abuse and arbitrary interferences with rights protected by the Convention.<sup>381</sup> Further in this respect, the Court has acknowledged that provisions on secret surveillance are to clearly indicate the discretion granted to authorities and the manner of its exercise.<sup>382</sup> This development has been described in this thesis by means of a model that articulates the legality condition in three layers.<sup>383</sup> These observations collectively provide a strong case for the development towards a structured and substantially strong legality condition.

---

<sup>379</sup> Nicoll et al., *supra* note 154, *passim*.

<sup>380</sup> Ch. 5.2.

<sup>381</sup> Ch. 5.2.3.5.

<sup>382</sup> *Ibid.*

<sup>383</sup> Ch. 6.2.

The second development may be demonstrated from an applicability point of view. The key driver in this respect is the extended applicability of principles originally developed for assessment of individual monitoring.<sup>384</sup> The case of *Liberty and others* confirmed the indications of this Court practice, when individual monitoring requirements were applied to the British general surveillance program that could intercept virtually any British citizen using telecommunications services.<sup>385</sup> As a result of this case the former individual requirements gained new ground as the field of application was significantly increased.<sup>386</sup> It is thus arguable that the applicability practice employed by the Court has contributed to the development towards an extended field of privacy protection.

Another important, somewhat specific, indication of contemporary development is the *Weber and Saravia* judgement.<sup>387</sup> The Court's review addressed several interesting legal aspects, such as the binding of data to its original purpose, data identification and transmission.<sup>388</sup> As the reasoning of the German Federal Constitutional Court has largely received endorsement by the European Court, it is unlikely that the Strasbourg machinery accepts a lower level of protection in equivalent circumstances.

Just as the Court's statements in the twin cases of *Huwig* and *Kruslin* appear to have influenced the subsequent development of minimum requirements, it is likely that some of the key surveillance issues of the future were touched upon in *Weber and Saravia*.<sup>389</sup> The case places central aspects of privacy and the rule of law to the fore, as the judgement concerns two contemporary trends, namely that states are adopting wide-ranging surveillance programs, while the border between national security and criminal procedure blurs.<sup>390</sup>

Who is to guarantee individuals' rights when digital footprints can become evidence by the mere push of a button? If the boundary continues to blur, and it becomes possible to institute criminal proceedings against literally anyone, on what basis will individuals then become criminals? Who is to defend for the rule of law when data banks are available and

---

<sup>384</sup> Ch. 5.2.3.4.

<sup>385</sup> The case of *Liberty and others*, *supra* note 60, paras 5, 63 and 64.

<sup>386</sup> For an analysis on the number of individuals affected by the British legislation and the subsequent impact on the accessibility criterion, see ch. 5.2.3.3

<sup>387</sup> Ch. 5.2.3.2.

<sup>388</sup> The German Federal Constitutional Court's assessment, *supra* note 198, *passim*.

<sup>389</sup> On the cases of *Huwig* and *Kruslin*, see *supra* notes 82 and 167, and *Cameron*, *supra* note 40, p. 105.

<sup>390</sup> For the former, see *supra* notes 12 and 13, for the latter, see *supra* note 362.

there is strong political pressure to take action? There are clearly several challenges on the privacy horizon.

The notion of privacy is diverse. As much as it brings benefits to the individual, it is a fundamental requirement in maintaining and developing democracy and pluralism.<sup>391</sup> Privacy naturally needs to be limited to some extent, for the pursuit of other virtues. The legality condition, which has been the main object of study of this thesis, has an important role to play when the limitation of rights is at stake. Its primary function is to oblige member states' surveillance programs to feature a threshold level of legislative quality. Indirectly it may contribute to the legal debate on the delicate balance between privacy and national security, by making visible the circumstances and conditions under which privacy can be encroached upon.

As a closing observation, well-intended measures against terrorism and international crime are not, as such, safeguards against the erosion of privacy. If these measures are employed without thorough preceding analysis, meticulous supervision and public transparency, secret surveillance may undermine civil society on the grounds of defending it.

---

<sup>391</sup> Cf. Waldo, *supra* note 2, pp. 371-2.

## Bibliography

### Articles

Bignami Francesca, *European versus American Liberty: A comparative privacy analysis of antiterrorism data mining*, Boston College Law Review, vol. 48, no. 3, 2007.

Cameron Iain, *Brottsbekämpning, rättssäkerhet och integritet – vissa internationella trender*, SvJT, vol. 1, 2007.

Cameron Iain, *European Court of Human Rights: April 2006 – March 2007*, European Public Law, vol. 13, no. 4, 2007.

Davis Robert N., *Striking the balance: National Security vs. Civil Liberties*, Brooklyn Journal of International Law, vol. 29, no. 1, 2003.

De Hert Paul, *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*, Utrecht Law Review, vol. 1, no. 1, 2005.

Ehrenkrona Carl Henrik, *Rättssäkerhetsbegreppet och Europakonventionen*, SvJT, vol. 1, 2007.

Koch Ida Elisabet & Vedsted-Hansen Jens, *International Human Rights and National Legislatures – Conflict or Balance?*, Nordic Journal of International Law, vol. 75, no. 1, 2006.

Ramberg Anne, *Tvångsmedel, rättssäkerhet och integritet – går det att förena?*, SvJT, vol. 1, 2007.

Schultz Mårten, *Skadeståndsrätten i de mänskliga rättigheternas tjänst*, JT, vol. 1, 2007/08.

Österdahl Inger, *Åke Green och missaktande men inte hatiskt tal*, SvJT, vol. 3, 2006.

### Literature

Acquisti Alessandro, *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton, 2008.

Cameron Iain, *An Introduction to the European Convention on Human Rights*, fifth edition, Iustus Förslag, Uppsala, 2006.

Cameron Iain, *National Security and the European Convention on Human Rights*, Iustus Förslag, Uppsala, 2000.

Danelius Hans, *Mänskliga rättigheter i europeisk praxis*, third edition, Norstedts Juridik, Stockholm, 2007.

Dutertre Gilles, *Key case law extracts – European Court of Human Rights*, Council of Europe Publishing, Strasbourg, 2003.

Fisher David I., *Mänskliga rättigheter – en introduktion*, second edition, Norstedts Juridik, Stockholm, 2001.

Harris D. J., O'Boyle M. & Warbrick C., *Law of the European Convention on human rights*, Butterworths, London, 1995.

Johnson Loch K., *America's Secret Power: The CIA in a Democratic Society*, Oxford University Press, Oxford, 1991.

Nicoll C., Prins J.E.J. & van Dellen M.J.M., *Digital Anonymity and the Law*, T M C Asser Press, The Hague, 2003.

Ovey Clare & White Robin, *European Convention on Human Rights*, forth edition, Oxford University Press, Oxford, 2006.

Strömberg Håkan & Lundell Bengt, *Sveriges författning*, 19th edition, Studentlitteratur, Lund, 2004.

Sottiaux Stefan, *Terrorism and the Limitation of Rights: The ECHR and the US Constitution*, Hart Publishing, Oxford and Portland, 2008.

Waldo James, *Engaging Privacy and information technology in a digital age*, National academic press, Washington D.C., 2007.

van Dijk Pieter, van Hoof Fried, van Rijn Arjen & Zwaak Leo, *Theory and Practice of the European Convention on Human Rights*, fourth edition, Intersentia, Antwerpten and Oxford, 2006.

Whitfield Diffie & Susan Eva Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, second edition, MIT Press, Cambridge, Massachusetts, 2007.

### **Preparatory legislative materials**

Prop. 1993/94:117, *Inkopporering av Europakonventionen och andra fri- och rättighetsfrågor*.

Prop. 2006/07:46, *Personuppgiftsbehandling hos Försvarsmakten och Försvarets Radioanstalt*.

Prop. 2006/07:63, *En anpassad försvarsunderrättelseverksamhet*.

### **Swedish Government Official Reports and Ministry publications series**

DS 2005:30, *En anpassad försvarsunderrättelseverksamhet*.

SOU 2003:30, *Försvarets radioanstalt – en översyn*.

SOU 2003:32, *Vår beredskap efter den 11 september*.

SOU 2004:32, *Informationssäkerhet i Sverige och internationellt – en översikt*.

SOU 2007:22, *Skyddet för den personliga integriteten - kartläggning och analys*.

**Other sources**

Encyclopædia Britannica Online, *Intelligence*, at <http://www.britannica.com/EBchecked/topic/289760/intelligence>, accessed on September 29<sup>th</sup> 2008.

Encyclopædia Britannica Online, *Information theory*, at <http://www.britannica.com/EBchecked/topic/287907/information-theory>, accessed on October 8<sup>th</sup> 2008.

The European Commission for democracy through law (Venice Commission), *Report on the democratic oversight of the security services*, Venice, 2007.

The FRA (The Swedish National Defence Radio Establishment), *Signalspanarna får viktiga roller på det elektroniska slagfältet*, at <http://www.fra.se/signalspaning.pdf>, accessed on October 8<sup>th</sup> 2008.

Parliament Defence Committee report, 200708;FöU15 *Lag om signalspaning m.m. (förnyad behandling)*.