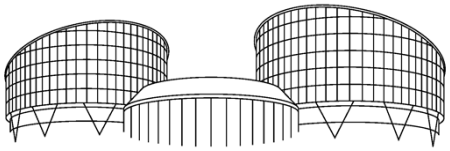

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF CENTRUM FÖR RÄTTVISA v. SWEDEN

(Application no. 35252/08)

JUDGMENT

STRASBOURG

19 June 2018

Referral to the Grand Chamber

04/02/2019

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

In the case of Centrum för rättvisa v. Sweden,

The European Court of Human Rights (Third Section), sitting as a Chamber composed of:

Branko Lubarda, *President,*
Helena Jäderblom,
Helen Keller,
Pere Pastor Vilanova,
Alena Poláčková,
Georgios A. Serghides,
Jolien Schukking, *judges,*

and Stephen Phillips, *Section Registrar,*

Having deliberated in private on 29 May 2018,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 35252/08) against the Kingdom of Sweden lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by Centrum för rättvisa on 14 July 2008.

2. The Swedish Government ("the Government") were represented by their Agent, Mr A. Rönquist, Ministry for Foreign Affairs.

3. The applicant alleged that Swedish legislation and practice in the field of signals intelligence have violated and continue to violate its rights under Article 8 of the Convention. It also complained that it has had no effective domestic remedy through which to challenge this violation.

4. On 1 November 2011 (admissibility) and 14 October 2014 (admissibility and merits) the application was communicated to the Government.

5. On 14 October 2014 the International Commission of Jurists, Norwegian Section, was granted leave to submit written comments, under Rule 44 § 3 of the Rules of the Court.

THE FACTS

I. INTRODUCTION

6. The applicant, Centrum för rättvisa, is a Swedish foundation which was established in 2002 and which has its seat in Stockholm. A not-for-profit organisation, its stated objective is to represent clients, in

litigation against the State and otherwise, who claim that their rights and freedoms under the Convention and under Swedish law have been violated. It also conducts education and research and participates in the general debate on issues concerning individuals' rights and freedoms. The applicant communicates on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax and asserts that a large part of that communication is particularly sensitive from a privacy perspective. Due to the nature of its function as a non-governmental organisation scrutinising the activities of State actors, it believes that there is a risk that its communication through mobile telephones and mobile broadband has been or will be intercepted and examined by way of signals intelligence. The applicant has not brought any domestic proceedings, contending that there is no effective remedy for its Convention complaints.

7. Signals intelligence can be defined as intercepting, processing, analysing and reporting intelligence from electronic signals. These signals may be processed to text, images and sound. The intelligence collected through these procedures may concern both the content of a communication and its associated communications data (the data describing, for instance, how, when and between which addresses the electronic communication is conducted). The intelligence may be intercepted over the airways – usually from radio links and satellites – and from cables. Whether a signal is transmitted over the airways or through cables is controlled by the communications service providers. A great majority of the traffic relevant for signals intelligence is cable-based. The term "signal carriers" refers to the medium used for transmitting one or more signals. Unless indicated in the following, the regulation of Swedish signals intelligence does not distinguish between the content of communications and their communications data or between airborne and cable-based traffic.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. Generally on signals intelligence

8. Foreign intelligence is, according to the Foreign Intelligence Act (*Lagen om försvarsunderrättelseverksamhet*; 2000:130), conducted in support of Swedish foreign, defence and security policy, and in order to identify external threats to the country. The activities should also assist in Sweden's participation in international security cooperation. Intelligence under the Act may only be conducted in relation to foreign circumstances (section 1(1)). The Government determines the direction of the activities; it also decides which authorities may issue more detailed directives and which authority is to conduct the intelligence activities (section 1(2) and 1(3)). The Government issues general tasking directives annually. Foreign intelligence may not be conducted for the purpose of solving tasks in the area of law

enforcement or crime prevention, which come under the mandate of the Police Authority, the Security Police and other authorities and which are regulated by different legislation. However, authorities that conduct foreign intelligence may support authorities dealing with law enforcement or crime prevention (section 4). Examples of such support are cryptanalysis and technical help on information security (preparatory works to amended legislation on foreign intelligence, prop. 2006/07:63, p. 136).

9. The collection of electronic signals is one form of foreign intelligence. It is regulated by the Signals Intelligence Act (*Lagen om signalspaning i försvarsunderrättelseverksamhet*; 2008:717), which entered into force on 1 January 2009. Several amendments were made to the Act on 1 December 2009, 1 January 2013, 1 January 2015 and 15 July 2016. Supplementary provisions are found in the Signals Intelligence Ordinance (*Förordningen om signalspaning i försvarsunderrättelseverksamhet*; 2008:923). The legislation authorises the National Defence Radio Establishment (*Försvarets radioanstalt*; henceforth "the FRA") to conduct signals intelligence (section 2 of the Ordinance compared to section 1 of the Act). During signals intelligence all cable-based cross-border communications are transferred to certain points of collection. No information is stored at these points and a limited amount of data traffic is transferred to the FRA by signals carriers (parliamentary committee report SOU 2016:45, p. 107) The FRA may conduct signals intelligence within the area of foreign intelligence only as a result of a detailed tasking directive issued by the Government, the Government Offices, the Armed Forces and, as from January 2013, the Security Police and the National Operative Department of the Police Authority (*Nationella operativa avdelningen i Polismyndigheten*; hereafter "NOA") (sections 1(1) and 4(1) of the Act) in accordance with the issuer's precise intelligence requirements. However, the direction of the FRA's "development activities" (see further paragraph 14 below) may be determined solely by the Government (section 4(2)). A detailed tasking directive determines the direction of the intelligence activities and may concern a certain phenomenon or situation, but it may not solely target a specific natural person (section 4(3)).

10. The mandate of the Security Police and the NOA to issue detailed tasking directives aims to improve these authorities' ability to obtain data about foreign circumstances at a strategic level concerning international terrorism and other serious international crime that may threaten essential national interests. At the time of introduction of the new rules, the Government stated in the preparatory works (prop. 2011/12:179, p. 19) that the mandate is in accordance with the prohibition on conducting signals intelligence for the purpose of solving tasks in the area of law enforcement or crime prevention.

11. According to the Foreign Intelligence Ordinance (*Förordningen om försvarsunderrättelseverksamhet*; 2000:131), a detailed tasking directive

shall include information about 1) the issuing authority, 2) the part of the Government's annual tasking directive it concerns, 3) the phenomenon or situation intended to be covered, and 4) the need for intelligence on that phenomenon or situation (section 2a).

B. Scope of application of signals intelligence

12. The purposes for which electronic signals may be collected as part of foreign intelligence are specified in the Signals Intelligence Act which provides that signals intelligence may be conducted only to survey 1) external military threats to the country, 2) conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations, 3) strategic circumstances concerning international terrorism or other serious cross-border crimes that may threaten essential national interests, 4) the development and proliferation of weapons of mass destruction, military equipment and other similar specified products, 5) serious external threats to society's infrastructure, 6) foreign conflicts with consequences for international security, 7) foreign intelligence operations against Swedish interests, and 8) the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy (section 1(2)).

13. These eight purposes are further elaborated upon in the preparatory works to the legislation (prop. 2008/09:201, pp. 108-109):

> "The purposes for which permits to conduct signals intelligence may be granted are listed in eight points. The first point concerns external military threats to the country. Military threats include not only imminent threats, such as threats of invasion, but also phenomena that may in the long term develop into security threats. Consequently, the wording covers the surveying of military capabilities and capacities in our vicinity.
>
> The second point comprises both surveying necessary to provide an adequate basis for a decision whether to participate in international peacekeeping or humanitarian missions and surveying performed during ongoing missions concerning threats to Swedish personnel or other Swedish interests.
>
> The third point refers to strategic surveying of international terrorism or other serious cross-border crime, such as drug or human trafficking of such severity that it may threaten significant national interests. The task of signals intelligence in relation to such activities is to survey them from a foreign and security policy perspective; the intelligence needed to combat the criminal activity operatively is primarily the responsibility of the police.
>
> The fourth point addresses the need to use signals intelligence to follow, among other things, activities relevant to Sweden's commitments in regard to non-proliferation and export control, even in cases where the activity does not constitute a crime or contravenes international conventions.
>
> The fifth point includes, among other things, serious IT-related threats emanating from abroad. That the threats should be of a serious nature means that they, for

example, should be directed towards vital societal systems for energy and water supply, communication or monetary services.

The sixth point refers to the surveying of such conflicts between and in other countries that may have consequences for international security. It may concern regular acts of war between states but also internal or cross-border conflicts between different ethnic, religious or political groups. The surveying of the conflicts includes examining their causes and consequences.

The seventh point signifies that intelligence activities conducted against Swedish interests can be surveyed through signals intelligence.

The eighth point provides the opportunity to conduct signals intelligence against foreign powers and their representatives in order to survey their intentions or actions that are of substantial importance to Swedish foreign, security or defence policy. Such activities may relate only to those who represent a foreign power. Through the condition "substantial importance" it is emphasised that it is not sufficient that the phenomenon is of general interest but that the intelligence should have a direct impact on Swedish actions or positions in various foreign, security or defence policy matters. ..."

14. The FRA may collect electronic signals also in order to monitor changes in the international signals environment, technical advances and signals protection and to develop the technology needed for signals intelligence (section 1(3)). This is regarded as "development activities" and, according to the relevant preparatory works (prop. 2006/07:63, p. 72), they do not generate any intelligence reports. However, the FRA may share experiences gained on technological issues with other authorities. Development activities usually do not focus on communications between individuals, though information on individuals' identities may be intercepted.

15. Signals intelligence conducted on cables may only concern signals crossing the Swedish border in cables owned by a communications service provider (section 2). Communications between a sender and receiver within Sweden may not be intercepted, regardless of whether the source is airborne or cable-based. If such signals cannot be separated at the point of collection, the recording of or notes about them shall be destroyed as soon as it becomes clear that such signals have been collected (section 2a).

16. Interception of cable-based signals is automated and must only concern signals that have been identified through the use of search terms. Such terms are also used to identify signals over the airways, if the procedure is automated. The search terms must be formulated in such a way that the interference with personal integrity is limited as far as possible. Terms directly relating to a specific natural person may only be used if this is of exceptional importance for the intelligence activities (section 3).

17. After the signals have been intercepted they are processed, which means that they are, for example, subjected to cryptanalysis or translation. Then the information is analysed and reported to the authority that gave the FRA the mission to collect the intelligence in question.

C. Authorisation of signals intelligence

18. For all signals intelligence, including the development activities, the FRA must apply for a permit to the Foreign Intelligence Court (*Försvarsunderrättelsedomstolen*). The application shall contain the mission request that the FRA has received, with information on the relevant detailed tasking directive and the need for the intelligence sought. Also, the signal carriers to which the FRA requires access have to be specified, along with the search terms or categories of search terms that will be used. Finally, the application must state the duration for which the permit is requested (section 4a).

19. A permit may only be granted if the mission is in accordance with the provisions of the Foreign Intelligence Act and the Signals Intelligence Act, if the purpose of the interception of signals cannot be met in a less interfering manner, if the mission can be expected to yield information whose value is clearly greater than the possible interference with personal integrity, if the search terms or categories of search terms are in accordance with the Signals Intelligence Act and if the application does not concern solely a specific natural person (section 5).

20. If granted, the permit shall specify the mission for which signals intelligence may be conducted, the signal carriers to which the FRA will have access, the search terms or categories of search terms that may be used, the duration of the permit and other conditions necessary to limit the interference with personal integrity (section 5a).

21. The FRA itself may decide to grant a permit, if the application for a permit from the Foreign Intelligence Court might cause delay or other inconveniences of essential importance for one of the specified purposes of the signals intelligence. If the FRA grants a permit, it has to report to the court immediately and the court shall without delay decide in the matter. The court may revoke or amend the permit (section 5b).

22. The composition of the Foreign Intelligence Court and its activities are regulated by the Foreign Intelligence Court Act (*Lagen om Försvarsunderrättelsedomstol*; 2009:966). The court consists of one president, one or two vice-presidents and two to six other members. The president is a permanent judge, nominated by the Judges Proposals Board (*Domarnämnden*) and appointed by the Government. The vice-presidents, who must be legally trained and have previous experience as judges, and the other members, who are required to have special expertise of relevance for the court's work, are appointed by the Government on four-year terms. The applications for signals intelligence permits are discussed during hearings, which may be held behind closed doors, if it is clear that information classified as secret would be exposed as a result of a public hearing. During the court's examination, the FRA as well as a privacy protection representative (*integritesskyddsombud*) are present. The representative, who

does not represent any particular person but the interests of individuals in general, monitors integrity issues and has access to the case file and may make statements. Privacy protection representatives are appointed by the Government for a period of four years and must be or have been permanent judges or attorneys. The court may hold a hearing and decide on an application without the presence of a representative only if the case is of such urgency that a delay would severely compromise the purpose of the application. The court's decisions are final.

D. The duration of signals intelligence

23. A permit may be granted for a specific period of time, maximum six months. An extension may, after a renewed examination, be granted for six months at a time (Signals Intelligence Act, section 5a).

E. Procedures to be followed for storing, accessing, examining, using and destroying the intercepted data

24. The Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten* (SIUN); see further paragraphs 36-40 below) oversees access to the signal carriers. Communications service providers are obliged to transfer cable-based signals crossing the Swedish borders to "collaboration points" agreed upon with the Inspectorate. The Inspectorate, in turn, provides the FRA with access to signal carriers in so far as such access is covered by a signals intelligence permit and, in so doing, implements the permits issued by the Foreign Intelligence Court (Chapter 6, section 19a of the Electronic Communications Act (*Lagen om elektronisk kommunikation*; 2003:389)). The Council on Legislation (*Lagrådet*), the body giving opinions on request by the Government or a Parliamentary committee on certain draft bills, has expressed the view that an interference with private life and correspondence presents itself already at this point, because of the State obtaining access to the telecommunications (prop. 2006/07:63, p. 172).

25. According to the Signals Intelligence Act, intercepted data must be destroyed immediately by the FRA if it 1) concerns a specific natural person and lacks importance for the signals intelligence, 2) is protected by constitutional provisions on secrecy for the protection of anonymous authors and media sources, 3) contains information shared between a suspect and his or her legal counsel and is thus protected by attorney-client privilege, or 4) involves information given in a religious context of confession or individual counselling, unless there are exceptional reasons for examining the information (section 7).

26. If communications have been intercepted between a sender and receiver who are both in Sweden, despite the prohibition on such

interception, they shall be destroyed as soon as the domestic nature of the communications has become evident (section 2a).

27. If a permit urgently granted by the FRA (see paragraph 21 above) is revoked or amended by the Foreign Intelligence Court, all intelligence collected which is thereby no longer authorised must be immediately destroyed (section 5b(3)).

28. The FRA Personal Data Processing Act (*Lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*; 2007:259) contains provisions on the treatment of personal data within the area of signals intelligence. The Act entered into force on 1 July 2007, with amendments made on 30 June 2009 and 15 February 2010. The purpose of the Act is to protect against violations of personal integrity (Chapter 1, section 2). The FRA shall ensure, *inter alia*, that personal data is collected only for certain expressly stated and justified purposes. Such purpose is either determined by the direction of the foreign intelligence activities through a detailed tasking directive or by what is necessary in order to follow changes in the signals environment, technical advances and signals protection. Also, the personal data treated has to be adequate and relevant in relation to the purpose of the treatment. No more personal data than what is necessary for that purpose may be processed. All reasonable efforts have to be made to correct, block and obliterate personal data that is incorrect or incomplete (Chapter 1, sections 6, 8 and 9).

29. Personal data may not be processed solely because of what is known of a person's race or ethnicity, political, religious or philosophical views, membership in a union, health or sexual life. If, however, personal data is treated for a different reason, this type of information may be used if it is absolutely necessary for the treatment. Information about a person's physical appearance must always be formulated in an objective way with respect for human dignity. Intelligence searches may only use the mentioned personal indicators as search terms if this is absolutely necessary for the purpose of the search (Chapter 1, section 11).

30. Personnel at the FRA who process personal data go through an official security clearance procedure and are subject to confidentiality in regard to data to which secrecy applies. They could face criminal sanctions if tasks relating to the processing of personal data are mismanaged (Chapter 6, section 2).

31. Personal data that has been subjected to automated processing shall be destroyed as soon as it is no longer needed (Chapter 6, section 1).

32. Further provisions on the treatment of personal data are laid down in the FRA Personal Data Processing Ordinance (*Förordningen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*; 2007:261). It provides, *inter alia*, that the FRA may keep databases for raw material containing personal data. Raw material is unprocessed information which has been

collected through automated treatment. Personal data in such databases shall be destroyed within one year from when it was collected (section 2).

F. Conditions for communicating the intercepted data to other parties

33. The intelligence collected shall be reported to the authorities concerned, as determined under the Foreign Intelligence Act (Signals Intelligence Act, section 8; see paragraphs 8-9 above).

34. The Government Offices, the Armed Forces, the Security Police, the NOA, the Inspectorate of Strategic Products (*Inspektionen för strategiska produkter*), the Defence Material Administration (*Försvarets materialverk*), the Defence Research Agency (*Totalförsvarets forskningsinstitut*), the Civil Contingencies Agency (*Myndigheten för samhällsskydd och beredskap*) and the Swedish Customs (*Tullverket*) may have direct access to completed intelligence reports to the extent the FRA so decides (section 9 of the FRA Personal Data Processing Ordinance). However, to date, no decisions permitting direct access have been taken by the FRA.

35. Personal data may be communicated to other states or international organisations only if not prevented by secrecy and if necessary for the FRA to perform its activities within international defence and security cooperation. The Government may adopt rules or decide in a specific case to allow such communication of personal data also in other cases when necessary for the activities of the FRA (Chapter 1, section 17 of the FRA Personal Data Processing Act). The FRA may disclose personal data to a foreign authority or an international organisation if it is beneficial for the Swedish government (*statsledningen*) or Sweden's comprehensive defence strategy (*totalförsvaret*); information so communicated must not harm Swedish interests (section 7 of the FRA Personal Data Processing Ordinance).

G. Supervision of the implementation of signals intelligence

36. The Foreign Intelligence Act (section 5) and the Signals Intelligence Act (section 10) prescribe that an authority is to oversee the foreign intelligence activities in Sweden and verify that the FRA's activities are in compliance with the provisions of the Signals Intelligence Act. The supervisory authority – the Foreign Intelligence Inspectorate – is, among other things, tasked with monitoring the implementation of the Foreign Intelligence Act and the associated Ordinance and reviewing whether foreign intelligence activities are performed in compliance with the applicable directives (section 4 of the Foreign Intelligence Inspectorate Instructions Ordinance (*Förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*; 2009:969)). It shall also

review compliance with the Signals Intelligence Act by examining in particular the search terms used, the destruction of intelligence and the communication of reports; if an inspection reveals that a particular intelligence collection is incompatible with a permit, the Inspectorate may decide that the operation shall cease or that the intelligence shall be destroyed (section 10 of the Signals Intelligence Act). The FRA shall report to the Inspectorate the search terms which directly relate to a specific natural person (section 3 of the Signals Intelligence Ordinance).

37. The Foreign Intelligence Inspectorate is led by a board whose members are appointed by the Government on terms of at least four years. The president and the vice-president shall be or have been permanent judges. Other members are selected from candidates proposed by the party groups in the Parliament (section 10 (3) of the Signals Intelligence Act).

38. Any opinions or suggestions for measures arising from the Inspectorate's inspections shall be forwarded to the FRA, and if necessary also to the Government. The Inspectorate also submits annual reports on its inspections to the Government (section 5 of the Foreign Intelligence Inspectorate Instructions Ordinance), which are made available to the public. Furthermore, if the Inspectorate notices potential crimes, it shall report the matter to the Prosecution Authority (*Åklagarmyndigheten*), and, if deficiencies are discovered that may incur liability for damages for the State, a report shall be submitted to the Chancellor of Justice (*Justitiekanslern*). A report may also be submitted to the Data Protection Authority (*Datainspektionen*), which is the supervisory authority on the treatment of personal data by the FRA (section 15).

39. From the establishment of the Inspectorate in 2009 until and including 2017, the latest year covered by its annual reports, no inspections have revealed reasons to cease an intelligence collection or to destroy the results. During the same period, the Inspectorate submitted several opinions and suggestions to the FRA and one to the Government. In the annual reports, brief descriptions have been given of the 102 inspections undertaken at the FRA; they have included numerous detailed examinations of the search terms used, the destruction of intelligence, the communication of reports, the treatment of personal data and the overall compliance with the legislation, directives and permits relevant to the signals intelligence activities. For instance, an inspection in 2014 concerned a general review of the FRA's cooperation with other states and international organisations in intelligence matters. It did not give rise to any opinion or suggestion to the FRA. In 2017 the Inspectorate carried out a detailed inspection of the treatment by the FRA of personal data. The inspection concerned treatment of sensitive personal data in connection with strategic circumstances with regard to international terrorism and other serious cross-border crime threatening significant national interests. The inspection did not give rise to any opinion or suggestion. However, during that year, one opinion was

submitted to the Government following an inspection of whether the FRA's intelligence activities were carried out within the direction given. During the years 2009-2017 the Inspectorate found reason to make a report to another authority – the Data Protection Authority – on one occasion, concerning the interpretation of a legal provision. In its annual reports, the Inspectorate has noted that it has been given access to all the information necessary for its inspections.

40. The supervisory activities of the Foreign Intelligence Inspectorate have been audited by the National Audit Office (*Riksrevisionen*), an authority under Parliament. In a report published in 2015 the Office noted that the FRA had routines in place for handling the Inspectorate's opinions and that the supervision helped develop the activities of the FRA. Suggestions were dealt with in a serious manner and, when called for, gave rise to reforms. At the same time the Office criticised the Inspectorate's lack of documentation of inspections and that there were no clearly specified goals for the inspections.

41. Within the FRA there is a Privacy Protection Council tasked with continuously monitoring measures taken to ensure protection of personal integrity. The members are appointed by the Government. The Council shall report its observations to the FRA management or, if the Council finds reasons for it, to the Inspectorate (section 11 of the Signals Intelligence Act).

42. Further provisions on supervision are found in the FRA Personal Data Processing Act. The FRA shall appoint one or several data protection officers and report the appointment to the Data Protection Authority (Chapter 4, section 1). The data protection officer is tasked with independently monitoring that the FRA treats personal data in a legal and correct manner and point out any deficiencies. If deficiencies are suspected and no correction is made, a report shall be submitted to the Data Protection Authority (Chapter 4, section 2).

43. The Data Protection Authority, which is an authority under the Government, has on request access to the personal data that is processed by the FRA and documentation on the treatment of personal data along with the security measures taken in this regard as well as access to the facilities where personal data is processed (Chapter 5, section 2). If the Authority finds that personal data is or could be processed illegally, it shall try to remedy the situation by communicating its observations to the FRA (Chapter 5, section 3). It may also apply to the Administrative Court (*förvaltningsrätten*) in Stockholm to have illegally processed personal data destroyed (Chapter 5, section 4).

H. Notification of secret surveillance measures

44. If search terms directly related to a specific natural person have been used, he or she is to be notified by the FRA, according to the Signals Intelligence Act. The notification shall contain information on the date and purpose of the measures. Such notification shall be given as soon as it can be done without detriment to the foreign intelligence activities, but no later than one month after the signals intelligence mission has been concluded (section 11a).

45. However, the notification may be delayed if secrecy so demands, in particular defence secrecy or secrecy for the protection of international relations. If, due to secrecy, no notification has been given within a year from the conclusion of the mission, the person does not have to be notified. Furthermore, a notification shall not be given if the measures solely concern the conditions of a foreign power or the relationship between foreign powers (section 11b).

I. Remedies

46. The Signals Intelligence Act provides that the Foreign Intelligence Inspectorate, at the request of an individual, must investigate if his or her communications have been intercepted through signals intelligence and, if so, verify whether the interception and treatment of the information have been in accordance with law. The Inspectorate shall notify the individual that such an investigation has been carried out (section 10a). A request can be made by legal and natural persons regardless of nationality and residence. During the period 2010-2017, 132 requests were handled and no unlawfulness was established. In 2017, ten such requests were processed; in 2016 the number was 14. The Inspectorate's decision following a request is final.

47. Under the FRA Personal Data Processing Act, the FRA is also required to provide information upon request. Once per calendar year, an individual may demand information on whether personal data concerning him or her is being or has been processed. If so, the FRA must specify what information on the individual is concerned, from where it was collected, the purpose of the treatment and to which recipients or categories of recipients the personal data is or was reported. The information is normally to be given within one month from the request (Chapter 2, section 1). However, this right to information does not apply if disclosure is prevented by secrecy (Chapter 2, section 3).

48. Following a request from the individual who has had personal data registered, the FRA shall promptly correct, block or destroy such data that has not been processed in accordance with law. The FRA shall also notify any third party who has received the data, if the individual so requests or if

substantial harm or inconvenience could be avoided through a notification. No such notification has to be given if it is impossible or would involve a disproportionate effort (Chapter 2, section 4).

49. The FRA's decisions on disclosure and corrective measures in regard to personal data may be appealed against to the Administrative Court in Stockholm (Chapter 6, section 3).

50. The State is liable for damages following a violation of personal integrity caused by treatment of personal data not in accordance with the FRA Personal Data Processing Act (Chapter 2, section 5). A request for damages shall be submitted to the Chancellor of Justice.

51. In addition to the above remedies, laid down in the legislation relating to signals intelligence, Swedish law provides for a number of other means of scrutiny and complaints mechanisms. The Parliamentary Ombudsmen (*Justititeombudsmannen*) supervise the application of laws and regulations in public activities; courts and authorities are obliged to provide information and opinions at the request of the Ombudsmen (Chapter 13, section 6 of the Instrument of Government – *Regeringsformen*), including access to minutes and other documents. The Ombudsmen shall ensure, in particular, that the courts and authorities observe the provisions of the Instrument of Government on objectivity and impartiality and that citizens' fundamental rights and freedoms are not encroached upon in public activities (section 3 of the Parliamentary Ombudsmen Instructions Act – *Lagen med instruktion för Riksdagens ombudsmän*; 1986:765). The supervision, under which the Foreign Intelligence Court and the FRA come, is conducted by means of examining complaints from the public and through inspections and other investigations (section 5). The examination is concluded by a decision in which, although not legally binding, the opinion of the Ombudsman is given as to whether the court or authority has contravened the law or otherwise taken a wrongful or inappropriate action; the Ombudsman may also initiate criminal or disciplinary proceedings against a public official who has committed a criminal offence or neglected his or her duty in disregarding the obligations of the office (section 6).

52. With a mandate similar to the Parliamentary Ombudsmen, the Chancellor of Justice scrutinises whether officials in public administration comply with laws and regulations and otherwise fulfil their obligations (section 1 of the Chancellor of Justice Supervision Act – *Lagen om justitiekanslerns tillsyn*; 1975:1339). The Chancellor does so by examining individual complaints or conducting inspections and other investigations, which could be directed at, for instance, the Foreign Intelligence Court and the FRA. At the request of the Chancellor, courts and authorities are obliged to provide information and opinions as well as access to minutes and other documents (sections 9 and 10). The decisions of the Chancellor of Justice are similar in nature to the decisions of the Parliamentary Ombudsmen, including their lack of legally binding power. By tradition, however, the

opinions of the Chancellor and the Ombudsmen command great respect in Swedish society and are usually followed (see *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 118, ECHR 2006-VII). The Chancellor has the same power as the Ombudsmen to initiate criminal or disciplinary proceedings (sections 5 and 6).

53. The Chancellor of Justice is also authorised to determine complaints and claims for damages directed against the State, including compensation claims for alleged violations of the Convention. The Supreme Court and the Chancellor of Justice have developed precedents in recent years, affirming that it is a general principle of law that compensation for Convention violations can be ordered without direct support in Swedish statute to the extent that Sweden has a duty to provide redress to victims of Convention violations through a right to compensation for damages (see *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, §§ 58-62 and 67, 20 December 2016, with further references). On 1 April 2018, through the enactment of a new provision – Chapter 3, section 4 – of the Tort Liability Act (*Skadeståndslagen*; 1972:207), the right to compensation for violations of the Convention was codified.

54. In addition to its above-mentioned supervisory functions under the Foreign Intelligence Inspectorate Instructions Ordinance and the FRA Personal Data Processing Act (see paragraphs 38, 42 and 43 above), the Data Protection Authority is generally entrusted with protecting individuals against violations of their personal integrity through the processing of personal data, under the Act with Supplementary Provisions to the EU General Data Protection Regulation (*Lagen med kompletterande bestämmelser till EU:s dataskyddsförordning*) which entered into force on 25 May 2018, the same day as the new EU regulation it supplements (paragraph 81 below). In regard to the signals intelligence conducted by the FRA – which falls outside the competence of the EU and is thus not regulated by Community law – the Personal Data Act (*Personuppgiftslagen;* 1998:204) continues to apply, although it is otherwise replaced by the new EU Regulation and the supplementary act. It gives the Data Protection Authority the same general supervisory task. In performing this task, the Authority may receive and examine individual complaints.

J. Secrecy at the FRA

55. The Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslagen*; 2009:400) contains a specific provision on the FRA's signals intelligence activities. Secrecy applies to information on an individual's personal or economic circumstances, unless it is evident that the information can be disclosed without the individual concerned or any other person closely related to him or her being harmed. The presumption is for secrecy (Chapter 38, section 4).

56. According to the Act, secrecy also generally applies to foreign intelligence activities in regard to information concerning another State, international organisation, authority, citizen or legal person in another State, if it can be presumed that a disclosure will interfere with Sweden's international relations or otherwise harm the country (Chapter 15, section 1).

57. Secrecy further applies to information on activities related to the defence of the country or the planning of such activities or to information that is otherwise related to the country's comprehensive defence strategy, if it can be presumed that a disclosure will harm the country's defence or otherwise endanger national security (Chapter 15, section 2).

58. Information which is protected by secrecy under the Public Access to Information and Secrecy Act may not be disclosed to a foreign authority or an international organisation unless 1) such disclosure is permitted by an express legal provision (cf. section 7 of the FRA Personal Data Processing Ordinance, paragraph 34 above), or 2) the information in an analogous situation may be communicated to a Swedish authority and the disclosing authority finds it evident that the communication of the information to the foreign authority or the international organisation is consistent with Swedish interests (Chapter 8, section 3 of the Act).

K. The reports of the Data Protection Authority

59. On 12 February 2009 the Government ordered the Data Protection Authority to examine the handling of personal data at the FRA from an integrity perspective. In its report, published on 6 December 2010, the Authority stated that its conclusions were overall positive. Issues relating to the processing of personal data and to personal integrity were given serious consideration by the FRA and a considerable amount of time and resources were spent on creating routines and educating its personnel in order to minimise the risk of unwarranted interferences with personal integrity. Moreover, no evidence had been found which indicated that the FRA was handling personal data for purposes not authorised by the legislation in force (see paragraphs 12-14 and 28 above). However, the Authority noted, *inter alia*, that there was a need to improve the methods for separating domestic and cross-border communications. Even if the FRA had implemented mechanisms in that area, there was no guarantee that domestic communications were never intercepted, and, although the occasions had been very few, such communications had in fact been intercepted. The Authority further noted that the procedure for notification to individuals (paragraphs 44-45 above) had never been used by the FRA, due to secrecy.

60. A second report was issued by the Authority on 24 October 2016. Again, the Authority found no evidence that personal data had been collected for other purposes than those stipulated for the signals intelligence

activities. It also noted that the FRA continuously reviewed whether data intercepted was still needed for those purposes. A similar review was made concerning the carriers from which the FRA obtained intelligence. Moreover, there was nothing to indicate that the provisions on destruction of personal data had been disregarded (see paragraphs 25-27 above). However, the FRA was criticised for not adequately monitoring logs used to detect unwarranted use of personal data, a shortcoming that had been pointed out already in 2010.

L. The report of the Signals Intelligence Committee

61. On 12 February 2009 the Government also decided to appoint a committee predominantly composed of members of parliament, the Signals Intelligence Committee (*Signalspaningskommittén*), with the task of monitoring the signals intelligence conducted at the FRA in order to examine the implications for personal integrity. The report was presented on 11 February 2011 (*Uppföljning av signalspaningslagen*; SOU 2011:13). The Committee's examination had its main focus on signals intelligence conducted over the airways as such activities on cable-based traffic had not yet commenced on a larger scale.

62. The Committee concluded that concerns of personal integrity were taken seriously by the FRA and formed an integral part of the development of its procedures. It noted, however, that there were practical difficulties in separating domestic cable-based communications from those crossing the Swedish border. Any domestic communications that were not separated at the automated stage were instead separated manually at the processing or analysing stage. The Committee further observed that the search terms used for communications data were less specific than those used for interception of the content of a communication and that, consequently, a larger number of individuals could have such data stored by the FRA.

63. Another finding in the report was that the FRA's development activities (see paragraph 14 above) could lead to non-relevant communications being intercepted and possibly read or listened to by FRA personnel. However, the Committee noted that the development activities were directly essential for the FRA's ability to conduct signals intelligence. Moreover, information obtained through the development activities could be used in the regular intelligence activities only if such use conformed with the purposes established by law and the relevant tasking directives issued for the signals intelligence.

64. Like the Data Protection Authority (see paragraph 59 above), the Committee pointed out that, in reality, the obligation of the FRA to notify individuals that had been directly and personally subjected to secret surveillance measures was very limited due to secrecy; it concluded therefore that this obligation served no purpose as a guarantee for legal

certainty or against integrity interferences. The Committee found, however, that, in particular, the authorisation procedure before the Foreign Intelligence Court, in deciding on permits to conduct signals intelligence measures (paragraphs 18-22), and the supervisory functions performed by the Foreign Intelligence Inspectorate (paragraphs 24 and 36-40) and the Privacy Protection Council (paragraph 41) provided important protection for individuals' personal integrity. It noted, in this respect, that, although the Privacy Protection Council formed part of the FRA, it acted in an independent manner.

III. RELEVANT INTERNATIONAL AND EUROPEAN LAW

A. United Nations

65. Resolution no. 68/167, on The Right to Privacy in the Digital Age, adopted by the General Assembly on 18 December 2013, reads as follows:

> "The General Assembly,
>
> ...
>
> 4. *Calls upon* all States:
>
> ...
>
> (*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;
>
> (*d*) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ..."

B. Council of Europe

1. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and its Additional Protocol

66. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (CETS No. 108) was ratified by Sweden on 29 September 1982. It sets out standards for data protection in the sphere of automatic processing of personal data in the public and private sectors. It provides, in so far as relevant, as follows:

Preamble

"The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:"

Article 1 – Object and purpose

"The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."

Article 8 – Additional safeguards for the data subject

"Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

Article 9 – Exceptions and restrictions

"1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

..."

Article 10 – Sanctions and remedies

"Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

67. The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181), ratified by Sweden on the latter date, provides as follows:

Article 1 – Supervisory authorities

"1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

..."

Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

"1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:

a. if domestic law provides for it because of:

– specific interests of the data subject, or

– legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law."

2. *Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services*

68. Recommendation No. R (95) 4 of the Committee of Ministers on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, adopted on 7 February 1995, reads, *inter alia*, as follows:

"2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:

a. the exercise of the data subject's rights of access and rectification;

b. in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;

c. storage or destruction of such data.

If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference."

3. *Report of the Venice Commission*

69. In December 2015 the European Commission for Democracy through Law – "the Venice Commission" – published its "Report on the Democratic Oversight of Signals Intelligence Agencies". The Commission noted, at the outset, the value that bulk interception could have for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones. However, it also noted that intercepting bulk data in transmission, or requirements that telecommunications companies store and then provide telecommunications content data or metadata to law-enforcement or security agencies involved an interference with the privacy and other human rights of a large proportion of the population of the world. In this regard, the Venice Commission considered that the main interference with privacy occurred when stored personal data was accessed and/or processed by the agencies. For this reason, the computer analysis

(usually with the help of selectors) was one of the important stages for balancing personal integrity concerns against other interests.

70. According to the report, the two most significant safeguards were the authorisation process (of collection and access) and the oversight process. It was clear from the Court's case-law that the latter must be performed by an independent, external body. While the Court had a preference for judicial authorisation, it had not found this to be a necessary requirement. Rather, the system had to be assessed as a whole, and where independent controls were absent at the authorisation stage, particularly strong safeguards had to exist at the oversight stage. In this regard, the Venice Commission considered the example of the system in the United States, where authorisation was given by the Foreign Intelligence Surveillance Court. However, it noted that despite the existence of judicial authorisation, the lack of independent oversight of the court's conditions was problematic.

71. Similarly, the Commission observed that notification of the subject of surveillance was not an absolute requirement of Article 8 of the Convention. In this regard, a general complaints procedure to an independent oversight body could compensate for non-notification.

72. The report also considered internal controls to be a "primary safeguard". In this regard, recruitment and training were key issues; in addition, it was important for the agencies to build in respect for privacy and other human rights when promulgating internal rules.

73. The report also considered the position of journalists. It accepted that they were a group which required special protection, since searching their contacts could reveal their sources (and the risk of discovery could be a powerful disincentive to whistle-blowers). Nevertheless, it considered there to be no absolute prohibition on searching the contacts of journalists, provided that there were very strong reasons for doing so. It acknowledged, however, that the journalistic profession was not one which was easily identified, since NGOs were also engaged in building public opinion and even bloggers could claim to be entitled to equivalent protections.

74. Finally, the report briefly considered the issue of intelligence sharing, and in particular the risk that States could thereby circumvent stronger domestic surveillance procedures or any legal limits which their agencies might be subject to as regards domestic intelligence operations. It considered that a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques.

C. European Union

1. Charter of Fundamental Rights of the European Union

75. Articles 7, 8 and 11 of the Charter provide as follows:

Article 7 – Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 – Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

Article 11 – Freedom of expression and information

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected."

2. EU directives relating to protection and processing of personal data

76. The Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), adopted on 24 October 1995, regulated for many years the protection and processing of personal data within the European Union. As the activities of member States regarding public safety, defence and State security fall outside the scope of Community law, the Directive did not apply to these activities (Article 3(2)).

77. The Privacy and Electronic Communications Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector), adopted on 12 July 2002, states, in recitals 2 and 11:

"(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the

State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms."

The Directive further provides, *inter alia*, the following:

Article 1 – Scope and aim

"1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law."

Article 15 – Application of certain provisions of Directive 95/46/EC

"1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

78. On 15 March 2006 the Data Retention Directive (Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) was adopted. It provided, *inter alia*, as follows:

Article 1 - Subject matter and scope

"1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network."

Article 3 – Obligation to retain data

"1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

..."

3. Case-law of the Court of Justice of the European Union (CJEU) on data protection

79. In *Digital Rights Ireland v Minister for Communications & Others*, (cases C-293/12 and C-594/12, judgment of 8 April 2014), the CJEU declared invalid Directive 2006/24/EC. The CJEU noted that, even though the directive did not permit the retention of the content of the communication, the traffic and location data covered by it might allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained. Accordingly, the obligation on providers of publicly available electronic communications services or of public communications networks to retain those data and the access of the national authorities to the data constituted an interference with the right to respect for private life and communications and the right to protection of personal data guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights. While the interference satisfied an objective of general interest, namely to contribute to the fight against serious crime and terrorism and thus, ultimately, to public security, it failed to satisfy the requirement of proportionality. The protection of the fundamental right to respect for private life required, according to the court's settled case-law, that derogations and limitations in relation to the protection of personal data could apply only in so far as was strictly necessary. The directive covered, however, in a generalised manner, all persons and all means of electronic communication as well as all communications data without any differentiation, limitation or exception being made in the light of the

objective of fighting against serious crime. It therefore entailed an interference with the fundamental rights of practically the entire European population, even to persons for whom there was no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, the directive did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. By simply referring to serious crime, as defined by each member State in its national law, the directive failed to lay down any objective criterion by which to determine which offences might be considered to be sufficiently serious to justify such an extensive interference with the rights enshrined in Articles 7 and 8 of the Charter. Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued. The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the rights in Articles 7 and 8 of the Charter, without having laid down clear and precise rules governing the extent of the interference and ensuring that it was actually limited to what was strictly necessary. Moreover, the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.

80. In joined cases *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* (cases C-203/15 and C-698/15, judgment of 21 December 2016), the CJEU (Grand Chamber) dealt, firstly, with the issue of a provider of electronic communications services having refused to retain data under Swedish legislation that had given effect to the now invalid Directive 2006/24/EC. The CJEU stated, *inter alia*, the following:

> "107. National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.
>
> 108. However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.
>
> 109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing

minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary. ...

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

112. Having regard to all of the foregoing, ... Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication."

The CJEU also examined a question by the Court of Appeal (England & Wales) (Civil Division) as to whether, in the *Digital Rights* judgment, the Court had interpreted Article 7 or 8 of the Charter in such a way as to expand the scope conferred on Article 8 of the Convention by the European Court of Human Rights. The CJEU stated:

"127. As a preliminary point, it should be recalled that, whilst, as Article 6(3) [of the Treaty on European Union] confirms, fundamental rights recognised by the [Convention] constitute general principles of EU law, the [Convention] does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law ... .

128. Accordingly, the interpretation of Directive 2002/58, which is at issue in this case, must be undertaken solely in the light of the fundamental rights guaranteed by the Charter ... .

129. Further, it must be borne in mind that the explanation on Article 52 of the Charter indicates that paragraph 3 of that article is intended to ensure the necessary consistency between the Charter and the [Convention], 'without thereby adversely affecting the autonomy of Union law and ... that of the Court of Justice of the European Union' (judgment of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84,

paragraph 47). In particular, as expressly stated in the second sentence of Article 52(3) of the Charter, the first sentence of Article 52(3) does not preclude Union law from providing protection that is more extensive then the [Convention]. It should be added, finally, that Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the [Convention].

130. However, in accordance with the Court's settled case-law, the justification for making a request for a preliminary ruling is not for advisory opinions to be delivered on general or hypothetical questions, but rather that it is necessary for the effective resolution of a dispute concerning EU law ... .

131. In this case, in view of the considerations set out, in particular, in paragraphs 128 and 129 of the present judgment, the question whether the protection conferred by Articles 7 and 8 of the Charter is wider than that guaranteed in Article 8 of the ECHR is not such as to affect the interpretation of Directive 2002/58, read in the light of the Charter, which is the matter in dispute in the proceedings in Case C-698/15.

132. Accordingly, it does not appear that an answer to the second question in Case C-698/15 can provide any interpretation of points of EU law that is required for the resolution, in the light of that law, of that dispute.

133. It follows that the second question in Case C-698/15 is inadmissible."

The CJEU ruled as follows:

"1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

3. The second question referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible."

4. The General Data Protection Regulation

81. On 25 May 2018 the General Data Protection Regulation (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

and repealing Directive 95/46/EC) entered into force. Like the Directive it replaced, the Regulation does not apply to State activities concerning public safety, defence and State security (Article 2(2)).

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

82. The applicant complained that that Swedish state practice and legislation concerning signals intelligence had violated and continued to violate its right to respect for private life and correspondence. The complaint concerned three time periods: from 2002 to 1 January 2009, from 1 January 2009 to 1 December 2009 and from 1 December 2009 onwards. The applicant invoked Article 8 of the Convention, which reads as follows:

> "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."

A. Admissibility

83. The Government questioned whether the applicant had exhausted all domestic remedies available and left it for the Court to determine the exhaustion issue. They further submitted that the applicant could not claim to be a victim of the alleged violation of Article 8. With regard to private life, the Government disputed that such a right was afforded to legal persons. In any event, they argued that the complaint was manifestly ill-founded.

84. In regard to the Government's first objection, the Court notes, as explained below (see paragraphs 171-177), that there is, in practice, no remedy which provides detailed grounds in its response to a complainant who suspects that he or she has had his communications intercepted. Furthermore, the Government have not pointed to any individual effective remedy that would have to be exhausted for the purposes of Article 35. The Court therefore finds that the applicant was not required to bring any domestic proceedings and accordingly rejects the objection concerning the exhaustion of domestic remedies.

85. As regards private life, the Court has previously held that it may be open to doubt whether a legal person can have a private life within the

meaning of Article 8. However, it can be said that its mail and other communications are covered by the notion of "correspondence" which applies equally to communications originating from private and business premises. Moreover, applicants who are legal persons may fear that they are subjected to secret surveillance and it has accordingly been accepted that they may claim to be victims (see *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 60, 28 June 2007, with further references). It is therefore appropriate to examine the complaint under the right to respect for the applicant's correspondence.

86. Considering that the Government's objection on victim status is closely linked to the substance of the applicant's complaint, it must be joined to the merits.

87. The Court further notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The applicant's victim status and the existence of an interference

(a) The parties' submissions

88. The Government submitted that the applicant could not claim to be a victim of a violation of the Convention by the mere existence of legislation concerning signals intelligence. The aggregate of control mechanisms, supervisory elements and remedies available constituted sufficient safeguards against abuse of the FRA's competence to conduct signals intelligence. Furthermore, the possibility that the applicant had been subject to signals intelligence was virtually non-existent.

89. The applicant disagreed with the Government and remarked, with reference to the case of *Kennedy v. the United Kingdom* (no. 26839/05, 18 May 2010), that its victim status was based on the risk of secret surveillance measures having been applied.

(b) The Court's assessment

90. In the *Roman Zakharov v. Russia* judgment ([GC], no. 47143/06, § 171, ECHR 2015), which concerned covert interception of mobile telephone communications, the Court, adopting the *Kennedy* approach, clarified the conditions under which an applicant can claim to be a victim of a violation of Article 8 without having to prove that secret surveillance measures have in fact been applied to him or her specifically. Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or

legislation permitting such measures, if the following conditions are satisfied.

91. Firstly, regard will be had to the scope of the legislation permitting secret surveillance measures through an examination of whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted.

92. Secondly, the availability of remedies at the national level will be taken into account; the degree of scrutiny will depend on the effectiveness of such remedies. Where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances, the menace of surveillance can be claimed in itself to restrict free communication through postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto*, is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were actually applied to him or her.

93. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he or she is able to show that, due to the specific personal situation, he or she is potentially at risk of being subjected to such measures.

94. The Court considers that the contested legislation on signals intelligence institutes a system of secret surveillance that potentially affects all users of, for example, mobile telephone services and the internet, without their being notified about the surveillance. Also, as concluded above (see paragraph 84), no domestic remedy provides detailed grounds in response to a complainant who suspects that he or she has had his communications intercepted. In these circumstances, the Court considers an examination of the relevant legislation *in abstracto* to be justified.

95. The applicant is therefore entitled to claim to be the victim of a violation of the Convention, even though it is unable to allege that it has been subjected to a concrete measure of interception. For the same reasons, the mere existence of the contested legislation amounts in itself to an interference with the exercise of the applicant's rights under Article 8. The Court therefore dismisses the Government's objection concerning the applicant's lack of victim status.

2. The temporal scope of the Court's examination

96. As already mentioned, the applicant has complained about three different time periods, arguing that each period is characterised by a different legal regime.

97. In other cases where the law has been reviewed *in abstracto* and amendments have been made to the legislation while the application was pending, the Court has limited itself to reviewing Convention compliance of the law in force at the time of its examination (see, for example, *Association for European Integration and Human Rights and Ekimdzhiev*, cited above; *Iordachi and Others v. Moldova*, no. 25198/02, 10 February 2009; and *Roman Zakharov*, cited above).

98. As stated above, the Court's task is not to examine measures that have "directly affected" the applicant, but to review the relevant Swedish law and practice *in abstracto*. The Swedish legislation has been amended on many occasions since the application was lodged with the Court, also since the start of the third time period on 1 December 2009. It cannot be the task of the Court, when reviewing the law *in abstracto*, to examine compatibility with the Convention before and after every single legislative amendment. The review will therefore focus on the Swedish legislation as it stands at the time of the present examination.

3. The justification of the interference

(a) General principles

99. The Court reiterates that any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim. The following general principles have been collated in *Roman Zakharov* (see §§ 228-236 of that judgment and the further references listed therein).

100. The wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects (*Roman Zakharov*, § 228).

101. The Court has held on several occasions that the reference to "foreseeability" in the context of interception of telephone communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance cannot mean that an individual should be able to foresee when the authorities are likely to intercept communications so that he or she can adapt his or her conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risk of arbitrariness is evident. It is therefore essential to have

clear, detailed rules on interception of telephone communications, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances and conditions which give public authorities the power to resort to such measures (*Roman Zakharov*, § 229).

102. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (*Roman Zakharov*, § 230).

103. In its case-law on secret measures of surveillance in criminal investigations, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: a description of the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of the measures; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed (*Roman Zakharov*, § 231).

104. As to the question whether an interference has been "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's rights under Article 8, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. It has to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the

"interference" to what is "necessary in a democratic society" (*Roman Zakharov*, § 232).

105. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control normally offering the best guarantees of independence, impartiality and a proper procedure (*Roman Zakharov*, § 233).

106. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to a remedy by the individual concerned unless he or she is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, that any person who suspects that his or her communications are being or have been intercepted can apply to an appropriate body, so that the latter's jurisdiction does not depend on a notification having been given to the subject who has had communications intercepted (*Roman Zakharov*, § 234).

107. Having found an interference of the applicant's rights under Article 8 § 1, in examining the justification for the interference under Article 8 § 2, the Court needs to determine whether the contested legislation itself is in conformity with the Convention (*Roman Zakharov*, § 235). In cases where the legislation permitting secret surveillance is contested, the matter of the lawfulness of the interference is closely related to the question whether the "necessity" requirement has been complied with and it is therefore appropriate to address these two issues jointly. The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, but must also ensure that secret surveillance measures are applied only when "necessary in a democratic

society", in particular by providing for adequate and effective safeguards and guarantees against abuse (*Roman Zakharov*, § 236).

(b) Existing case-law on the bulk interception of communications

108. The Court has considered the Convention compatibility of regimes which expressly permit the bulk interception of communications on two occasions: first in *Weber and Saravia v. Germany* ((dec.), no. 54934/00, ECHR 2006-XI), and then in *Liberty and Others v. the United Kingdom* (no. 58243/00, 1 July 2008).

109. In *Weber and Saravia* the applicants complained about the process of strategic monitoring under the amended G10 Act, which authorised the monitoring of international wireless telecommunications. Signals emitted from foreign countries were monitored by interception sites situated on German soil with the aid of certain catchwords which were listed in the monitoring order. Only communications containing these catchwords were recorded and used. Having particular regard to the six "minimum safeguards" (see paragraph 103 above), the Court considered that there existed adequate and effective guarantees against abuses of the State's strategic monitoring powers. It therefore declared the applicants' Article 8 complaints to be manifestly ill-founded.

110. In *Liberty and Others* the Court was considering the regime under the Interception of Communications Act 1985 which allowed the executive to intercept communications passing between the United Kingdom and an external receiver. At the time of issuing an interception warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted material which he considered should be examined. On the face of the 1985 Act, external communications sent to or from an address in the United Kingdom could only be included in the certificate if the Secretary of State considered it necessary for the prevention or detection of acts of terrorism. Otherwise, the legislation provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered that this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom's economy. The Court held that the domestic law at the relevant time did not indicate with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.

(c) Application of these principles to the facts of the case

111. It has not been disputed by the parties that the Swedish signals intelligence, in its present structure, has a basis in domestic law.

Furthermore, the Court considers it clear that the measures permitted by Swedish law pursue legitimate aims in the interest of national security by supporting Swedish foreign, defence and security policy and identifying external threats to the country. It therefore remains to be ascertained whether the domestic law is accessible and contains adequate and effective safeguards and guarantees to be considered "foreseeable" and "necessary in a democratic society".

112. The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106). In *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation.

113. Nevertheless, it is evident from the Court's case-law over several decades that all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation (see, for example, *Klass and Others v. Germany*, 6 September 1978, Series A no. 28; *Kennedy*, cited above; *Roman Zakharov*, cited above, and *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016). Therefore, while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower. In this regard, the Court has identified six minimum safeguards that both bulk interception and other interception regimes must incorporate in order to be sufficiently foreseeable to minimise the risk of abuses of power (see paragraph 103 above).

114. Accordingly, adapting these minimum safeguards where necessary to reflect the operation of a bulk interception regime dealing exclusively with national security issues, the following assessment of the interference established (see paragraph 95 above) will address, in turn, the accessibility of the domestic law, the scope and duration of signals intelligence, the authorisation of the measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted

data, the arrangements for supervising the implementation of the measures, any notification mechanisms and the remedies provided for by national law.

(i) Accessibility of domestic law

115. The Court finds that all legal provisions relevant to signals intelligence have been officially published and are accessible to the public, a fact that has not been questioned by the applicant.

(ii) Scope of application of signals intelligence

(α) The parties' submissions

116. The applicant submitted that, whereas the conduct against which signals intelligence could be directed had clear affinities to various criminal offences, for instance crimes against the security of the nation, the same could not be said for the FRA's development activities. The latter activities allegedly permitted bulk collection of data, including large amounts of communications data, without regard to the requirement that interception be ordered only in regard to certain specific offences. The applicant further emphasised that, since 1 January 2013, the Security Police and the NOA have been given a mandate to issue more detailed tasking directives for signals intelligence. Since the general tasks of these two authorities were crime prevention and investigation there was a risk that signals intelligence was being conducted outside the scope of foreign intelligence activities.

117. The Government submitted that the FRA's development activities were as rigorously regulated – and subject to supervision to the same extent – as signals intelligence in general. The Government also opposed the claim that signals intelligence could be used to investigate crimes, as the law did not permit such use of signals intelligence.

(β) The Court's assessment

118. The Court reiterates that the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures (see paragraph 103 above).

119. The requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. At the same time, it must be emphasised that in matters affecting fundamental rights it would be contrary to the rule of law for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and

the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 247, with further references).

120. The Signals Intelligence Act stipulates eight purposes for which signals intelligence may be conducted (see paragraph 12 above). Although some of these purposes are generally framed, they are further elaborated upon in the preparatory works (paragraph 13), which is an essential source of Swedish legislation. The Court finds that these eight purposes are adequately indicated (cf. *Roman Zakharov*, cited above, §§ 246 and 248).

121. It is of further importance that signals intelligence conducted on fibre optic cables may only concern communications crossing the Swedish border in cables owned by a communications service provider. Communications between a sender and a receiver in Sweden may not be intercepted, regardless whether the source is airborne or cable-based.

122. It is true that the FRA may also intercept signals as part of its development activities which, it appears, mainly concern the collection of communications data. Such collection is made in order to monitor changes in the international signals environment and to develop the FRA's own signals intelligence technology, and may lead to data not relevant for the regular foreign intelligence being intercepted and read. Also, the search terms used for interception of communications data – whether part of the development activities or not – are less specific than those used for interception of the content of a communication (see paragraph 62 above). However, as noted by the Signals Intelligence Committee (paragraph 63), the development activities are essential for the proper functioning of the foreign intelligence and the information thereby obtained may be used in the regular foreign intelligence only if such use is in conformity with the purposes established by law and the applicable tasking directives. Moreover, the provisions applicable to the regular foreign intelligence work are also relevant to the development activities and to any interception of communications data, including the requirement of a permit issued by the Foreign Intelligence Court (paragraph 18). It is further of relevance in this context that, in its 2010 and 2016 reports, the Data Protection Authority found no evidence that personal data had been collected for other purposes than those stipulated for the signals intelligence activities (paragraphs 59-60). In these circumstances, the Court is satisfied that the scope of application of the development activities is sufficiently demarcated.

123. As from 1 January 2013, the Security Police and the NOA have been authorised to issue detailed tasking directives for signals intelligence. While, as pointed out by the applicant, the tasks of these authorities include crime prevention and investigation, section 4 of the Foreign Intelligence Act clearly excludes the use of foreign intelligence to solve tasks in the area of law enforcement or crime prevention (see paragraph 8 above).

124. Consequently, the Court finds that the law indicates the scope of mandating and performing signals intelligence conferred on the competent authorities and the manner of its exercise with sufficient clarity.

(iii) Duration of secret surveillance measures

(α) The parties' submissions

125. The applicant submitted that the legislation satisfied the minimum requirements in terms of duration of the permit.

126. The Government held that the Signals Intelligence Act clearly regulated the maximum duration of a permit and the conditions under which a permit could be renewed.

(β) The Court's assessment

127. The Court has held that it is not unreasonable to leave the overall duration of interception to the discretion of the relevant domestic authorities which have competence to issue and renew interception warrants, provided that adequate safeguards exist, such as a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled (see *Roman Zakharov*, cited above, § 250).

128. As regards the first two safeguards, the Signals Intelligence Act stipulates that a permit may be granted for a maximum of six months and that it may be extended, following a new examination, for six months at a time (see paragraph 23 above). The examination preceding a renewal must be understood as encompassing a full review by the Foreign Intelligence Court as to whether the conditions set out in section 5 of the Act are still met (paragraph 19). The Act thus gives clear indications of the period after which the permit will expire and of the conditions under which it can be renewed.

129. In respect of the third safeguard, the circumstances in which interception must be discontinued, the legislation is not equally clear. There is no provision obliging the FRA, the authorities mandated to issue detailed tasking directives or the Foreign Intelligence Court to cancel a signals intelligence mission if the conditions for it have ceased to exist or the measures themselves are no longer necessary (cf. *Klass and Others*, cited above, § 52; and *Kennedy*, cited above, § 161).

130. Nevertheless, notwithstanding that the relevant legislation is less clear with regard to the third safeguard, it must be borne in mind that any permit is valid for a maximum of six months and that a renewal requires a review as to whether the conditions are still met. Furthermore, although the Foreign Intelligence Inspectorate is not tasked with inspecting every signals intelligence permit, it may decide that an intelligence interception shall cease, if during an inspection it is evident that the interception is not in

accordance with a permit (see paragraph 36 above). The Court also has regard to the fact that the permits in question concern the collection of intelligence related to threats to national security and are not targeting individuals suspected of criminal conduct, in which case the need for specific provisions on the cancellation of permits would have been more prominent. Moreover, as noted by the Data Protection Authority (paragraph 60), the FRA continuously reviews whether the specific personal data it has intercepted is still needed for its signals intelligence activities. In these circumstances, the Court is satisfied that there are safeguards in place which adequately regulate the duration, renewal and cancellation of interception measures.

(iv) Authorisation of secret surveillance measures

(α) The parties' submissions

131. The applicant submitted that, although signals intelligence could not be conducted without prior authorisation by the Foreign Intelligence Court, the court's impartiality and independence from the Government could be questioned and its activities were covered by complete secrecy. Its hearings and decisions had never been made public. The same was true for information about the number of hearings, the number of permits granted or rejected, any reasoning of its decisions or the amount or type of search terms being used. As to the composition of the court, its members were elected for a limited period of time, except for the president.

132. The Government emphasised that all signals intelligence conducted required a permit from the Foreign Intelligence Court, including the FRA's development activities. The Government also stressed that the court was independent from Parliament and public authorities. Although its activities were governed by secrecy, a privacy protection representative was present to safeguard the interests of individuals.

(β) The Court's assessment

133. As the Court has previously held, the authorisation of telephone tapping by a non-judicial authority may be compatible with the Convention (see, for example, *Klass and Others*, cited above, § 51; and *Weber and Saravia*, cited above, § 115), provided that that authority is sufficiently independent from the executive (*Roman Zakharov*, cited above, § 258). However, the rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control normally offering the best guarantees of independence, impartiality and a proper procedure (*Klass and Others*, cited above, §§ 55 and 56). Prior judicial authorisation may serve to limit the authorities' discretion in interpreting the scope of mandating and

performing signals intelligence. Thus, a requirement of prior judicial authorisation constitutes an important safeguard against arbitrariness (*Roman Zakharov*, cited above, § 249). Nevertheless, prior authorisation of such measures is not an absolute requirement *per se*, because where there is extensive subsequent judicial oversight, this may counterbalance the shortcomings of the authorisation (*Szabó and Vissy*, cited above, § 77).

134. Under Swedish law, signals intelligence conducted by the FRA must be authorised in advance by the Foreign Intelligence Court. The president of the court is a permanent judge, whereas the vice president and other members are appointed by the Government on four-year terms. Neither Parliament nor the Government or other authorities may interfere with the court's decision-making, which is legally binding.

135. The main rule is that the court shall hold public hearings but, when secrecy applies, hearings may be held in private. As submitted by the applicant, and confirmed by the Government, the court's activities are in practice covered by complete secrecy. A hearing has never been open to the public and all decisions are confidential. As noted by the applicant, no information is disclosed to the public about the number of hearings, the number of permits granted or rejected, the reasoning of the court's decisions or the amount or type of search terms being used.

136. The Court is mindful of the fact that the nature of signals intelligence requires that surveillance is done in secret (see paragraph 101 above). It must therefore be accepted that, where there is a system of prior authorisation, sensitive aspects of the authorising body's activities are withheld from the public for as long as required in the individual case, in order not to defeat the purpose of the signals intelligence. However, such a procedure could only be accepted where there are adequate safeguards in place.

137. The Government have submitted that the lack of transparency is compensated by the presence of the privacy protection representative. He or she must be present during the court's examination, except in very urgent cases. The representative is either a present or former permanent judge or attorney and has access to all the case documents and may make statements. He or she does not appear on behalf of any individual concerned by the signals intelligence permit at issue, but protects the interests of the general public.

138. The Court is of the view that, while the privacy protection representative cannot appeal against a decision by the Foreign Intelligence Court or report any perceived irregularities to the supervisory bodies, the presence of the representative at the court's examinations compensates, to a limited degree, for the lack of transparency concerning the court's proceedings and decisions.

139. More importantly, taking into account that proceedings and decisions relating to secret surveillance largely require secrecy, the Court

considers that what is essential for the protection of individuals' rights in the context of the regime under consideration is that the FRA's signals intelligence is subject to a system of prior authorisation whereby the FRA must submit for independent examination an application for a permit to conduct surveillance in respect of each intelligence collection mission. As an additional safeguard against abuse and arbitrariness, the task of examining whether the mission is compatible with applicable legislation and whether the intelligence collection is proportional to the resultant interference with personal integrity has been entrusted to a body whose presiding members are or have been judges. Furthermore, the supervision of the Foreign Intelligence Court is extensive as the FRA, in its applications, must specify not only the mission request in question and the need for the intelligence sought but also the signal carriers to which access is needed and the search terms – or at least the categories of search terms – that will be used (see paragraphs 18-20 above). The Court therefore considers that the judicial supervision performed by the Foreign Intelligence Court is of crucial importance in that it limits the FRA's discretion by interpreting the scope of mandating and performing signals intelligence.

140. As a final point under this heading, it should be noted that the FRA itself may decide to grant a permit, if it is feared that the application of a permit from the Foreign Intelligence Court might cause delay or other inconveniences of essential importance for one of the specified purposes of the signals intelligence. In this context the Court reiterates the need for safeguards to ensure that such emergency measures are used sparingly and only in justified cases (*Roman Zakharov*, cited above, § 266). As the legislation states that such a decision must be followed by an immediate notification to and a subsequent rapid review by the Foreign Intelligence Court where the permit may be changed or revoked, the Court finds this procedure acceptable (cf. *Szabó and Vissy*, cited above, § 81).

141. In light of the foregoing, the Court finds that the provisions and procedures relating to the system of prior court authorisation, on the whole, provide important guarantees against abuse.

(v) Procedures to be followed for storing, accessing, examining, using and destroying the intercepted data

(α) The parties' submissions

142. The applicant argued that the procedures in these aspects were regulated in only very broad terms. For example, there was no general obligation to destroy data.

143. The Government pointed out that the Foreign Intelligence Inspectorate was responsible for scrutinising the treatment and destruction of data in general and had a mandate to terminate surveillance and order the

destruction of data that had been collected in a way that was incompatible with a permit issued by the Foreign Intelligence Court.

(β) The Court's assessment

144. The Court notes that personnel at the FRA treating personal data are security cleared and, if secrecy applies to the personal data, subject to confidentiality. They are under an obligation to handle the personal data in a safe manner. Also, they could face criminal sanctions if tasks relating to the treatment of personal data are mismanaged (see paragraph 30 above). Furthermore, the FRA must ensure that personal data is collected only for certain expressly stated and justified purposes, determined by the direction of the foreign intelligence activities through tasking directives. The personal data treated also has to be adequate and relevant in relation to the purpose of the treatment. No more personal data than what is necessary for that purpose may be processed. All reasonable efforts have to be made to correct, block and obliterate personal data which is incorrect or incomplete in relation to the purpose (paragraph 28).

145. Contrary to the applicant's claim, there are several provisions regulating the situations when intercepted data has to be destroyed. For example, intelligence must be destroyed immediately if it 1) concerns a specific natural person and has been determined to lack importance for the purpose of the signals intelligence, 2) is protected by constitutional provisions of secrecy for the protection of anonymous authors or media sources, 3) contains information shared between a criminal suspect and his or her counsel and is thus protected by attorney-client privilege, or 4) involves information given in a religious context of confession or individual counselling, unless there are exceptional reasons for examining the information (see paragraph 25 above). Moreover, if communications have been intercepted between a sender and receiver both in Sweden, despite the ban on the interception of such communications, they must be destroyed as soon as their domestic nature has become evident (paragraph 26). Also, where a temporary permit granted by the FRA has been revoked by the Foreign Intelligence Court, all intelligence collected on the basis of that permit must be immediately destroyed (paragraph 27).

146. Although the FRA may maintain databases for raw material containing personal data up to one year, it has to be kept in mind that raw material is unprocessed information. That is, it has yet to be subjected to manual treatment. The Court accepts that it is necessary for the FRA to store raw material before it can be manually processed. At the same time, the Court stresses the importance of deleting such data as soon as it is evident that it lacks pertinence for a signals intelligence mission.

147. In sum, examining the legislation on storing, accessing, examining, using and destroying intercepted data, the Court is satisfied that it provides adequate safeguards against abuse of treatment of personal data and thus

serves to protect individuals' personal integrity (cf. *Roman Zakharov*, cited above, §§ 253-256; and *Kennedy*, cited above, §§ 162-164).

(vi) Conditions for communicating the intercepted data to other parties

(α) The parties' submissions

148. The applicant submitted that the conditions for communicating data left a large discretion to the FRA, for instance through the lack of specification as regards the foreign authorities and international organisations to whom data could be communicated.

149. The Government maintained that the procedures for communicating data, including the communication to other states and international organisations as part of Sweden's international cooperation, contained sufficient safeguards and that supervision was provided by the Foreign Intelligence Inspectorate.

(β) The Court's assessment

150. With regard to the communication of intercepted data to other parties, the purpose of signals intelligence naturally demands that it may be reported to concerned national authorities, in particular the authority which ordered the mission. Furthermore, given the context – the collection of intelligence on foreign circumstances that may have an impact on Swedish national security and other essential national interests as well as the country's participation in international security operations – it is evident that there must be a possibility of exchanging intelligence collected with international partners. Thus, the FRA Personal Data Processing Act allows the communication of personal data to other states or international organisations if necessary for the activities of the FRA within international defence and security cooperation and as long as it is not prevented by secrecy. Further discretion is given to the Government, which may decide to communicate personal data to states or organisations in other cases when necessary for the activities of the FRA, thus presumably in cases where such communication would otherwise be prevented by rules of secrecy. The FRA Personal Data Processing Ordinance adds that such disclosure is permitted for the benefit of the Swedish Government and Sweden's comprehensive defence strategy as long as it does not harm Swedish interests (see paragraph 35 above). The relevant provision of the Public Access to Information and Secrecy Act contains an exception to the rule of secrecy in relation to foreign authorities and international organisations in cases where an express legal provision allows disclosure or when the information in an analogous situation may be given to a Swedish authority and the disclosing authority finds it to be consistent with Swedish interests (paragraph 58). Thus, whereas national interests are taken into account, the legislation does not indicate that possible harm to the individual concerned must be

considered. Furthermore, the legislation only in very broad terms mentions that the data may be communicated to "other states or international organisations"; there is no provision requiring the recipient to protect the data with the same or similar safeguards as those applicable under Swedish law. Also the situation where data may be communicated – when necessary for "international defence and security cooperation" – opens up for a rather wide scope of discretion. In the Court's view, the mentioned lack of specification in the provisions regulating the communication of personal data to other states and international organisations gives some cause for concern with respect to the possible abuse of the rights of individuals. On the whole, however, the Court considers that the supervisory elements described below sufficiently counterbalance these regulatory shortcomings.

(vii) Supervision of the implementation of secret surveillance measures

(α) The parties' submissions

151. The applicant, pointing to the findings of the National Audit Office, submitted that the Foreign Intelligence Inspectorate's own documentation of its supervisory work was scarce and that the Inspectorate lacked specified goals.

152. The Government submitted that an assessment of the report of the National Audit Office had been communicated to Parliament. The Office's overall conclusion was that the Inspectorate had been given the necessary prerequisites to carry out its supervisory functions in an efficient and effective manner. The FRA had taken the Inspectorate's views seriously and implemented measures accordingly. As to the Inspectorate's goals, these were clearly specified in the legislation.

(β) The Court's assessment

153. The Court has found that, although it is in principle desirable to entrust supervisory control to a judge, supervision by a non-judicial body may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control (see *Roman Zakharov*, cited above, § 275, with further reference).

154. As to the requirement of independence, the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it has found sufficiently independent the bodies composed of members of Parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by Parliament or by the Prime Minister (see *Roman Zakharov*, cited above, § 278, with further references).

155. As regards the supervisory body's powers and competence, it is essential that it has access to all relevant documents, including closed materials, and that all those involved in interception activities have a duty to disclose to it any material required. Other important elements to take into account when assessing the effectiveness of the supervision are the supervisory body's powers with respect to any breaches detected and the possible public scrutiny of its activities. Moreover, it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples (see *Roman Zakharov*, cited above, §§ 281-283, with further references).

156. The members of the Foreign Intelligence Inspectorate are appointed by the Government on terms of at least four years and the president and vice-president are current or former permanent judges. The other members are suggested by the parliamentarian party groups (see paragraph 37 above). The Court, therefore, finds no reason to question the independence of the Inspectorate.

157. The Inspectorate shall examine in particular the search terms used, the destruction of intelligence and how reports are communicated; the FRA shall report to it the search terms which directly relate to a specific natural person (see paragraph 36 above). The Inspectorate has access to all relevant documents (paragraph 39). It is within its powers to decide that the collection of intelligence shall cease or that information collected shall be destroyed, if during an inspection it becomes evident that the collection has not been in accordance with a particular permit; though, as of yet, no such measure has proved necessary (paragraphs 36 and 39). The Inspectorate is also in charge of the signal carriers, which includes ensuring that the FRA is only provided with access to signal carriers insofar as such access is covered by the permit (paragraph 24). The Inspectorate is to forward to the FRA, and if needed to the Government, any opinions or suggestions for measures to which the inspections give rise (paragraph 38).

158. The Court considers that the supervision of the Foreign Intelligence Inspectorate is of particular value in ensuring that the provisions applicable to the activities of the FRA are respected and that, generally, signals intelligence is performed in a manner which offers adequate safeguards against abuse. The above-mentioned rules governing the work of the Inspectorate indicate that it has been given sufficient powers to carry out this task. Moreover, contrary to the applicant's claim, the Court understands the report of the National Audit Office as concluding that the Inspectorate has been able to carry out its supervisory task efficiently. The Office also found that the FRA has taken the Inspectorate's views and suggestions seriously and have implemented measures based on them (see paragraph 40 above). The Court is therefore satisfied that the Inspectorate's supervision is efficient, not only in theory but also in practice.

159. The Court also finds that the Inspectorate's activities are open to public scrutiny. Beyond the audit provided by the National Audit Office, the Inspectorate submits annual reports to the Government on its activities; these reports are available to the public (see paragraph 38 above).

160. As regards personal data, further supervisory functions are provided by the Data Protection Authority. The Authority has on request access to personal data that is processed, documentation on the treatment of personal data along with the security measures taken on such treatment and access to the facilities connected to the processing of personal data. If the Authority finds that personal data is or could be processed illegally, it shall take remedial action through remarks to the FRA. The Authority may also apply to an administrative court to have illegally processed personal data destroyed (see paragraph 43 above). The Authority's supervision led to reports published in 2010 and 2016, in which some aspects of the FRA's activities were criticised. Issues of personal data and personal integrity, however, were generally considered to have been dealt with in a satisfactory manner (paragraphs 59-60).

161. Having regard to the above, the Court finds that the supervisory elements provided by the Foreign Intelligence Inspectorate and the Data Protection Authority fulfill the requirements on supervision in general. Moreover, the Parliamentary Ombudsmen and the Chancellor of Justice have general supervisory responsibilities in regard to the FRA.

(viii) Notification of secret surveillance measures

(α) The parties' submissions

162. The applicant submitted that the obligation on the FRA to notify natural persons when search terms directly related to them had been used was void of any practical meaning, since notifications had never been made due to secrecy.

163. The Government confirmed that a notification had never been given by the FRA for reasons of secrecy, but submitted that this was compensated by the remedy according to which the Foreign Intelligence Inspectorate could check at the request of an individual whether his or her communication had been subject to signals intelligence.

(β) The Court's assessment

164. The Court reiterates that it may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods

and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned (see *Roman Zakharov*, cited above, § 287, with further references).

165. The Court, mindful of the fact that the applicant is not a natural person, notes that, in theory, the FRA is obliged to inform a natural person, if search terms directly related to him or her have been used, about when and why the collection took place. The person shall be notified as soon as it can be done without detriment to the foreign intelligence activities, but at the latest one month after the signals intelligence mission was concluded. However, the obligation to notify does not apply where secrecy applies. The parties, as well as the Data Protection Authority in its report of 6 December 2010 (see paragraph 59 above) and the Signals Intelligence Committee in its report of 11 February 2011 (paragraph 64), have confirmed that in practice a notification has never been made, due to secrecy. Thus, the Court agrees with the applicant that the obligation on the FRA to notify individuals lacks practical significance.

166. The Court has previously found that the absence of a requirement to notify the subject of interception of postal and telephone communications at any point in time or in any circumstances was incompatible with the Convention, in that it deprived the subject of the interception an opportunity to seek redress for unlawful interferences with his or her rights under Article 8 and rendered the remedies available under national law theoretical and illusory rather than practical and effective (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, §§ 90 and 91). By contrast, in the case of *Kennedy*, the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his or her communications were being or had been intercepted could complain about an unlawful interception to a tribunal, whose jurisdiction did not depend on notification to the subject that there had been an interception of his or her communications (*Kennedy*, cited above, § 167).

167. Taking into account that the requirement to notify the subject of secret surveillance measures is not applicable to the applicant and is, in any event, devoid of practical significance, the Court accordingly finds it pertinent to examine the issue of notification together with the remedies available in Sweden; two issues that are inextricably linked (see *Roman Zakharov*, cited above, § 286).

(ix) Available remedies

(α) The parties' submissions

168. The applicant submitted that persons who had availed themselves of the possibility to request an investigation by the Foreign Intelligence Inspectorate had received a standardised reply that no unlawful surveillance had taken place. The applicant also stressed that the Inspectorate had no power to order compensation to be paid. No complaints regarding signals intelligence conducted by the FRA had been received by the Data Protection Authority after 2009. In regard to the Parliamentary Ombudsmen, the Chancellor of Justice and the other remedies mentioned by the Government, the applicant did not see any prospects of success unless there was evidence to establish that an individual had in fact been subjected to unlawful interception.

169. The Government emphasised that Swedish legislation offered several remedies. Beyond the possibility for individuals to request the Foreign Intelligence Inspectorate to check if his or her communications had been intercepted, the FRA was obliged, upon request, to inform the individual if his or her personal data had been treated or not and to correct, block or destroy personal data that had not been processed in accordance with law. In addition, complaints could be addressed to the Parliamentary Ombudsmen and the Chancellor of Justice, who had the power to investigate that relevant laws had been properly applied and, in so doing, were entitled to have access to documents of courts and administrative authorities, including the Foreign Intelligence Court and the FRA. Although they could not render legally binding decisions, their opinions commanded great respect in Swedish society. Also the Data Protection Authority, aside from being the supervisory authority on the FRA's treatment of personal data, could examine individual complaints. Furthermore, it was possible for an individual to bring an action for damages, report a matter for prosecution and bring a claim for compensation for violations of the Convention.

170. The International Commission of Jurists, Norwegian Section, submitted that remedies were not available to non-Swedish citizens, despite the fact that Swedish signals intelligence was focused on communications crossing the Swedish border.

(β) The Court's assessment

171. As the Court noted above, in the case of *Kennedy* the absence of a requirement to notify the subject of interception was compatible with the Convention, because the jurisdiction of the tribunal where the interception could be challenged did not depend on a prior notification (see *Kennedy*, cited above, § 167). Under the Signals Intelligence Act, the Foreign Intelligence Inspectorate, at the request of an individual, investigates whether his or her communications have been intercepted through signals

intelligence. If so, the Inspectorate verifies whether the interception and treatment of the information was in accordance with law. The Inspectorate must notify the individual that an investigation has been carried out. A request can be made by legal and natural persons regardless of nationality and residence (see paragraph 46 above). The Inspectorate has the power to decide that the collection of intelligence shall cease or that the intelligence shall be destroyed (paragraph 36).

172. Like in the *Kennedy* case, the Court is therefore satisfied that the remedy offered by the Foreign Intelligence Inspectorate is not dependent on prior notification. Although the Inspectorate may decide on the discontinuation of intelligence collection or the destruction of intelligence, unlike in *Kennedy*, it may not order compensation to be paid. However, with regard to compensation *per se*, the Court is mindful that there is an effective remedy in Sweden in that compensation from the State can be sought through the Chancellor of Justice or the domestic courts (see paragraph 53 above).

173. The Inspectorate examines if the individual's communications have been intercepted using signals intelligence. However, that examination is limited to the question whether or not the collection of intelligence was in accordance with law. The individual cannot obtain information whether his or her communications have actually been intercepted, only if there has been any unlawfulness. As pointed out by the applicant, the Inspectorate does not give any reasons for its conclusions reached on the issue of lawfulness. In contrast, the Court noted in *Kennedy* that the publication of the tribunal's legal rulings enhanced the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see *Kennedy*, cited above, § 167). Moreover, as the decision of the Inspectorate is final, an individual who is not satisfied with the response from the Inspectorate may not seek review by, for instance, making an appeal to a court.

174. As to the remedies available directly through the FRA, the Court makes the following observations. The FRA is, upon request, required to inform an individual whether personal data concerning him or her has been processed. A request may be submitted once per calendar year. If such data has been treated, the FRA must specify what information on the individual is concerned, from where it was collected, the purpose of the treatment and to which recipients or categories of recipients the personal data has been reported (see paragraph 47 above). The Court notes that such an obligation is well-tailored to lower suspicion and concern among the general public that secret surveillance measures are being abused.

175. However, like the notification requirement, there is no obligation on the FRA to give information if secrecy applies to it. While the FRA's decisions may be appealed against to the Administrative Court in Stockholm (see paragraph 49 above), the Court has to assume that, like with other aspects of the FRA's activities, strict secrecy applies and, therefore, no

information on personal data is given to requesting individuals. In the absence of examples provided by the Government that illustrate the effectiveness of this remedy, the Court cannot find that it has practical importance. Furthermore, the FRA's procedure to correct, block or destroy personal data (paragraph 48) is dependent on the individual's knowledge that personal data has been registered and the nature of that data. Therefore, that remedy must be deemed to be ineffective in practice.

176. The Court notes, however, that Swedish law provides for several remedies of a general nature, in particular the possibility of addressing individual complaints to the Parliamentary Ombudsmen and the Chancellor of Justice (see paragraphs 51-53 above). These two institutions examine whether courts and authorities and their officials comply with laws and regulations and fulfil their obligations, not the least in regard to citizens' fundamental rights and freedoms. They are thus authorised to scrutinise the work of the courts and authorities involved in signals intelligence activities and there appears to be no impediment preventing an individual from introducing a complaint about an interference of privacy rights. The two institutions have the right of access to documents and other materials for the performance of their scrutiny. While their decisions are not legally binding, their opinions command great respect in Sweden. They also have the power to initiate criminal or disciplinary proceedings against public officials for actions taken in the discharge of their duties. As regards the Chancellor of Justice, it is also of relevance that a practice has developed in the last several years according to which the Chancellor may receive and resolve individual compensation claims for alleged violations of the Convention (paragraphs 53 and 172).

Moreover, the Court notes that the Data Protection Authority may receive and examine individual complaints under the Personal Data Act (paragraph 54).

177. To sum up, the Court observes that the Swedish remedies available for complaints relating to secret surveillance do not include the recourse to a court, save for an appeal against the FRA's decisions on disclosure and corrective measures, which remedies the Court have as such found to be ineffective. Furthermore, there does not appear to be a possibility for an individual to be informed of whether his or her communications have actually been intercepted or, generally, to be given reasoned decisions. Thus, in regard to the final stage of supervision of signals intelligence measures – reviews requested by individuals after the measures have been carried out – the Swedish system does not offer the same guarantees in these respects as the scrutiny in the United Kingdom, examined in the *Kennedy* case.

178. Nevertheless, there are several remedies by which an individual may initiate an examination of the lawfulness of measures taken during the operation of the signals intelligence system, notably through requests to the

Foreign Intelligence Inspectorate, the Parliamentary Ombudsmen and the Chancellor of Justice. In the Court's view, the aggregate of remedies, although not providing a full and public response to the objections raised by a complainant, must be considered sufficient in the present context, which involves an abstract challenge to the signals intelligence regime itself and does not concern a complaint against a particular intelligence measure. In reaching this conclusion, the Court attaches importance to the earlier stages of supervision of the regime, including the detailed judicial examination by the Foreign Intelligence Court of the FRA's requests for permits to conduct signals intelligence and the extensive and partly public supervision by several bodies, in particular the Foreign Intelligence Inspectorate.

(x) Conclusion

179. The Court is mindful of the potentially harmful effects that the operation of a signals intelligence scheme may have on the protection of privacy. Nevertheless, the Court acknowledges the importance for national security operations of a system such as the one examined in the present case. It notes, in this respect, the similar conclusions drawn by the Venice Commission (see paragraph 69 above). Having regard to the present-day threats being posed by global terrorism and serious cross-border crime as well as the increased sophistication of communications technology, the decision to set up a bulk interception regime in order to identify such threats was one which fell within the respondent State's margin of appreciation. As noted above (paragraph 112), in deciding on the type of regime necessary, the margin afforded was a wide one.

180. As noted simultaneously, the State's discretion in operating the interception regime is more narrow. When examining the Swedish system of signals intelligence *in abstracto*, the Court has had regard to the relevant legislation and the other information available in order to assess whether, on the whole, there are sufficient minimum safeguards in place to protect the public from abuse. While the above assessment has disclosed some areas where there is scope for improvement – notably the regulation of the communication of personal data to other states and international organisations (see paragraph 150 above) and the practice of not giving public reasons following a review of individual complaints (paragraphs 173 and 177) – the Court is of the opinion that the system reveals no significant shortcomings in its structure and operation. The regulatory framework has been reviewed several times, in order to expand the use of signals intelligence but also, more importantly, with the aim to enhance protection of privacy. It has developed in such a way that it minimises the risk of interference with privacy and compensates for the lack of openness. In particular, the scope of the signals intelligence measures and the treatment of intercepted data are clearly defined in law, the authorisation procedure is detailed and entrusted to a judicial body and there are several independent

bodies tasked with the supervision and review of the system. The Court's finding that the system reveals no significant shortcomings is the result of an examination *in abstracto* and does not preclude a review of the State's liability under the Convention where, for example, the applicant has been made aware of an actual interception.

181. Accordingly, making an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security, the Court finds that the Swedish system of signals intelligence provides adequate and sufficient guarantees against arbitrariness and the risk of abuse. The relevant legislation meets the "quality of law" requirement and the "interference" established can be considered as being "necessary in a democratic society". Furthermore, the structure and operation of the system are proportionate to the aim sought to be achieved.

There has accordingly been no violation of Article 8 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

182. The applicant complained that it has had no effective domestic remedy through which to challenge the violation of its rights under Article 8 of the Convention. The applicant relied on Article 13 of the Convention, which reads as follows:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

183. The Government contested that argument.

184. Having regard to the findings under Article 8 (see, in particular, paragraph 178 above), the Court considers that, although the present complaint is closely linked to the complaint under Article 8 and therefore has to be declared admissible, it raises no separate issue under Article 13 of the Convention.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Joins* to the merits the Government's objection regarding the applicant's lack of victim status and *declares* the application admissible;

2. *Dismisses* the Government's above-mentioned objection;

3. *Holds* that there has been no violation of Article 8 of the Convention;

4. *Holds* that there is no need to examine separately the complaint under Article 13 of the Convention.

Done in English, and notified in writing on 19 June 2018, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Stephen Phillips Registrar	Branko Lubarda President