CENTRUM FÖR RÄTTVISA

Stockholm, 3 May 2019

IN THE EUROPEAN COURT OF HUMAN RIGHTS
(GRAND CHAMBER):

Application no. 35252/08

CENTRUM FÖR RÄTTVISA

("**Applicant**")

v.

SWEDEN

("**Government**")

THE APPLICANT'S FURTHER WRITTEN OBSERVATIONS ON ADMISSIBILITY AND THE MERITS

CONTENTS

INTRODUCTION

1. At the invitation of the President of the Grand Chamber of the European Court of Human Rights (the "**Grand Chamber**" and the "**Court**" respectively), the Applicant makes the following further written submissions in the case of *Centrum för rättvisa v. Sweden*, application no. 35252/08 (the "**Case**").

2. As requested, these submissions provide a detailed outline of the Applicant's position on the complaints it raises. They also provide responses to the Court's questions to the parties in its letter dated on 7 March 2019 ("**Court's Questions**").

SUMMARY OF SUBMISSIONS

3. This Case presents the Grand Chamber with the opportunity to clarify what minimum safeguards under Article 8 of the European Convention om Human Rights (the **"Convention**") should govern the use of bulk interception of electronic signals for national security purposes. Specifically, the Applicant respectfully requests that the Grand Chamber:

    a) finds that the main elements of a bulk interception regime must be set out in *statute law*, in order to ensure that the legislative branch is involved in the necessary

balancing between different interests and to promote foreseeability, transparency, and public trust;

b) finds that a requirement of *prior judicial authorisation* constitutes a mandatory minimum safeguard against the arbitrary or abusive use of bulk interception surveillance powers by the executive branch,

c) re-examines the Chamber's exclusion of the *reasonable suspicion* requirement laid out in *Roman Zakharov v. Russia*[1] from the mandatory minimum safeguards for bulk interception regimes, and requires that were reasonable suspicion is not feasible, comparable procedural safeguards are afforded to bulk interception regimes. In cases where there are no defined targets at the initial point of data collection, the authorising body (i) must nevertheless be required to meet a similiar *materiality or relevance threshold* to use personal data as selectors, and (ii) must ensure there are appropriate safeguards insofar as individuals are targeted in the subsequent analysis and reporting stages of the surveillance activities;

d) affirms that suitable supervision, notification, and remedy measures constitute required minimum safeguards for a bulk interception regime; and

e) develops the minimum safeguards governing communication of data to foreign governments and international organisations particularly in order to prevent the circumvention of domestic legal limits and important domestic safeguards.

4. In the Applicant's submission, the Swedish's bulk interception regime meets neither the existing Convention standards nor the updated standards suggested above. In answer to the Court's Questions, the Applicant submits the following:

a) **Question 1:** The mere existence of the legislation authorising the Swedish signals intelligence regime constitutes an interference with the Applicant's rights under Article 8 § 1 of the Convention. Each stage of the signals intelligence process (interception, storage, use, and the communication of data) further constitutes interferences with those rights, presenting distinct privacy risks.

b) **Question 2:** The interference is not in accordance with the law and necessary in a democratic society as *per* Article 8 § 2. There are compelling reasons for the Court to find that modern large-scale bulk interception regimes, such as the Swedish

[1] *Roman Zakharov v. Russia* [GC], no. 47143/06, § 260, ECHR 2015.

signals intelligence regime, are inherently disproportionate and incompatible with the Convention. Should the Court, however, find that operating a large-scale foreign intelligence bulk interception regime falls within the margin of appreciation afforded to Contracting States to the Convention ("**Contracting States**"), the Swedish signals intelligence regime fails to satisfy several of the minimum safeguards required under Article 8, namely:

- there is no clear indication in law of the circumstances in which an interception warrant must be cancelled, and specifically, no obligation;
- the scope of the prior judicial authorisation review is insufficient; there is no requirement of reasonable suspicion, the materiality threshold is insufficient and there is no possibility for the authorising body to assess the necessity of the intended subsequent use of collected data;
- the supervisory bodies largely lack the necessary power to render legally binding decisions; and
- there are no effective remedies for individuals who suspect that their communications have been unlawfully intercepted.

c) **Question 2a:** Should the Court find that the operation of a bulk interception regime falls within Contracting States' margin of appreciation, it must not hesitate in setting down robust minimum safeguards. These must be appropriately formulated, and, where necessary, updated to address the distinct privacy risks and technical realities of a modern bulk interception regime.

d) **Question 2b:** Safeguards can exist without being made public, provided that they are subject to independent oversight and insofar as the main elements of the secret surveillance regime are set out in statute law. The requirement of statute law is vital in order to ensure that the legislature is involved in the necessary balancing between different interests and to promote foreseeability, transparency, and public trust.

e) **Question 2c:** Article 8 § 2 requires supervision and review by an independent body, capable of rendering legally binding decisions, when the surveillance is first ordered, while it is being carried out, and after it has been terminated. When surveillance is first ordered, the Court should require that it be subject to prior *judicial* authorisation.

f) **Question 2d:** The same Convention standards should apply to both intercepted communications and related communications data. The Swedish legislation, however, does not differentiate between them.

g) **Question 2e:** The system applicable in Sweden as regards individual requests for review does not meet the relevant Convention requirements. There are no possibilities for individuals to obtain effective review and appropriate redress. The Government has not established that the available remedies are effective.

h) **Question 3:** Contracting States' responsibilities under Article 8 of the Convention extend to communication of intercepted data to foreign governments and international organisations. Those responsibilities include an obligation to take reasonable steps to ensure that the receiving party protects the data with similar safeguards as applies to the Contracting State. The Swedish signals intelligence regime does not contain any such obligation and fails to satisfy the applicable Convention standards.

5. For these reasons, the Court is invited to find that the Applicant's rights under Article 8 and Article 13 of the Convention have been violated.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

A. Admissibility

6. The Applicant submits that the Chamber's decision to declare the application admissible is firmly grounded in the Court's established case law on admissibility in secret surveillance cases [2], and that there are no grounds for the Grand Chamber to depart from the Chamber's finding.

B. Merits: The Swedish signals intelligence regime

1 The existence of an interference

7. Question 1 of the Court's Questions states:

[2] Chamber Judgment, §§ 86–87 and 94–95.

> "Has there been an interference with the Applicant's rights under Article 8 § 1 of the Convention on account of the 'bulk interception' of communications in Sweden?
>
> In particular, the parties are invited to clarify at which stage(s) the interception and processing of information is capable of affecting the rights of concrete individuals or organisations; and to describe the manner in which the individuals or organisations are affected at the stage(s) identified."

8. The Government has not contested that the Swedish signals intelligence regime is capable of interfering with Article 8 of the Convention.[3] The Chamber found, in accordance with the Court's established case law, that the mere existence of the contested legislation amounts in itself to an interference with the Applicant's rights under Article 8.[4] This finding is sufficient for the purposes of the *in abstracto* review of the present Case.

9. Every key stage of the signals intelligence process comprises further concrete interferences with the rights protected under Article 8.[5] However, as individuals and organisations are not notified under the Swedish regime when their communications are being intercepted, stored, used or communicated, the manner in which they are concretely affected at each stage do not differ from the individual's practical perspective.

10. From the individual's practical perspective, it is mainly the "chilling effect" of the knowledge that the Government covertly monitors all cross-border communications that has a negative impact on the enjoyment of the rights under Article 8. This in turn risk hampering personal development, professional secrecy, exploration and expression of identity and development of relationships.[6]

---

[3] Observations of the Government of Sweden on Admissibility and Merits of 8 May 2015 in *Centrum för rättvisa v. Sweden*, para. 59.

[4] Chamber Judgment, § 95; see also *inter alia Roman Zakharov*, cited above, § 179; *Szabó and Vissy v. Hungary*, no. 37138/14, § 33, 12 January 2016; *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 78, ECHR 2006-XI; and *Klass and Others v. Germany*, 6 September 1978, § 41, Series A no. 28.

[5] *Cf. Malone v. the United Kingdom*, 2 August 1984, § 64, Series A no. 82; and *Kopp v. Switzerland*, 25 March 1998, § 53, Reports of Judgments and Decisions 1998-II (interception); *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II; and *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116 (storage); *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Brito Ferrinho Bexiga Villa-Nova v. Portugal*, no. 69436/10, § 44, 1 December 2015 (use, including consultation); and *Rotaru*, cited above, § 43; and *Leander*, cited above, § 48 (communication of data).

[6] *Cf. S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 66, ECHR 2008; *Brito Ferrinho Bexiga Villa-Nova*, cited above, § 44; and *Amann*, cited above, § 65.

2 The justification of the interference

2.1 General principles

11. Article 8 § 2 of the Convention states that an interference with the rights in Article 8 § 1 can only be justified if certain conditions are met.

12. Firstly, the measure must be in accordance with the law. In order for a measure to be "in accordance with the law", it must not only have a basis in domestic law, but the law itself must be compatible with the rule of law and uphold certain quality requirements. The law must be *accessible* to those with whom it is concerned and *foreseeable* as to its effects.[7] Secondly, the measure must pursue one or more of the legitimate aims stipulated in Article 8 § 2 Convention. Thirdly, the measure must be necessary in a democratic society in order to achieve the legitimate aim pursued.

2.2 The Court's case law on secret surveillance

13. The Court has developed a series of key principles that govern how the abovementioned requirements are to be interpreted and applied in the secret surveillance context, including cases involving the secret interception of communications.

2.2.1 Foreseeability in a secret surveillance context

14. Firstly, the Court has held that in secret surveillance cases, the "foreseeability" requirement does not mean that the law needs to enable individuals to pinpoint exactly when they are likely to be subject to surveillance, so as to allow them to adapt their conduct accordingly. Such a requirement would risk undermining the efficacy of secret surveillance operations. Nevertheless, in order to protect against the arbitrary or abusive use of surveillance powers by the executive or another authorised body, the law must be "sufficiently clear" so as to "give citizens an adequate indication as to the circumstances and conditions which give public authorities the power to resort to such measures".[8]

[7] See, *e.g.*, *Roman Zakharov,* cited above, § 228; *S and Marper,* cited above, § 95; and *Rotaru,* cited above, § 52.

[8] Chamber Judgment, § 101 with reference to *Roman Zakharov,* cited above, § 229. See also *Malone,* cited above, § 67.

15. The applicable law must also "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".[9]

2.2.2 Secret surveillance and the margin of appreciation

16. Secondly, in determining whether secret surveillance measures undertaken for purposes of, *inter alia*, national security are necessary in a democratic society, the Court will afford Contracting States a certain margin of appreciation in their selection of the means by which to pursue such legitimate aims.[10]

17. This margin of appreciation, however, remains "subject to European supervision" and requires Contracting States to ensure that they implement "adequate and effective guarantees against abuse" given the risk that "secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it".[11]

2.2.3 The development of "minimum safeguards"

18. Thirdly, if the Court considers a secret surveillance regime to fall within the margin of appreciation, it then proceeds to assess whether the surveillance regime has a basis in law, its accessibility, and then conducts a joint analysis of the foreseeability and necessity requirements with reference to a series of minimum safeguards.

(i) The evolution of the minimum safeguards

19. In *Klass and Others v. Germany* (1978), the Court recognised the need for secret surveillance regimes to contain "adequate and effective guarantees" against abuse as a restriction on the States margin of appreciation.[12]

20. In *Huvig v. France* (1990), the Court held that French laws on phone tapping were not sufficiently detailed or clear to meet the quality of law requirements under Article 8 § 2. Whilst containing a number of safeguards, the Court pointed out that the law failed to

---

[9] Chamber Judgment, § 102 with reference to *Roman Zakharov,* cited above*,* § 230. See also *Malone,* cited above, § 68.

[10] See, *e.g.*, *Szabó and Vissy*, cited above, § 57; and *Roman Zakharov*, cited above, § 232.

[11] See, *e.g.*, *Szabó and Vissy*, cited above, § 57; *Roman Zakharov*, cited above, § 232; and *Weber and Saravia,* cited above, § 106.

[12] *Klass and Others,* cited above, § 50.

specify, for instance, the categories of people liable to have their phones tapped; the nature of offences that may give rise to a phone interception order; a requirement to have limits on the duration of the phone tapping; the procedure for drawing up the summary reports of the intercepted conversation; the procedure for keeping the entirety of the conversations intact for examination by the judge and the defence; and the circumstances when the intercepted material must be erased or destroyed.[13] The Court then applied these safeguards in several subsequent phone-tapping cases.[14]

21. In *Weber and Saravia v. Germany* (2006), the Court examined an untargeted communication interception regime for the first time. It drew reference from the *Huvig* phone-tapping safeguards and applied them, albeit in an adapted form. Reference to the procedure for drawing up summary reports was adapted to the "procedure to be followed for examining, using, and storing the data obtained". Similarly, the need for precautions for keeping communications intact for judicial examination was widened to "precautions to be taken when communicating the data to other parties".[15]

22. The Court subsequently applied the safeguards as formulated in *Weber* in several targeted interception cases,[16] and when assessing the United Kingdom's untargeted interception regime in *Liberty and Others v. United Kingdom* (2008).[17]

(ii) A joint analysis: the safeguards according to Roman Zakharov

23. In its more recent case law on the interception of communications, the Court has taken to viewing the foreseeability and necessity requirements as "closely related" and analysed them jointly with reference to the minimum safeguards.[18] In the Grand Chamber case of *Roman Zakharov v. Russia* (2015), the Court structured its analysis around the following:

---

[13] *Huvig v. France*, 24 April 1990, §§ 33–35, Series A no. 176-B.

[14] See *Kruslin v. France*, 24 April 1990, § 35, Series A no. 176-A; *Valenzuela Contreras v. Spain*, 30 July 1998, § 59, *Reports of Judgments and Decisions* 1998-V; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003.

[15] *Weber and Saravia*, cited above, § 95.

[16] See, *e.g.*, *Iordachi and Others v. Moldova*, no. 25198/02, § 39, 10 February 2009; and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 76, 28 June 2007.

[17] *Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 62–69, 1 July 2008.

[18] See, *e.g.*, *Kvasnica v. Slovakia*, no. 72094/01, § 84, 9 June 2009; *Kennedy v. the United Kingdom*, no. 26839/05, § 155, 18 May 2010; and *Roman Zakharov*, cited above, § 236.

a) scope of application of secret surveillance measures (in particular, the nature of offences giving rise to an interception order and a definition of the categories of people liable to have their communications intercepted);
b) duration of the secret surveillance measures;
c) procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data;
d) authorisation of interceptions (in particular, the prior authorisation of an interception order and access by the authorities to the communications);
e) supervision of the implementation of secret surveillance measures; and
f) notification of interception of communications and available remedies.[19]

2.3 Assessing the compatibility of modern bulk interception regimes with the Convention

24. Question 2a of the Court's Questions states:

> "*To what extent should the standards developed in the Court's case-law on secret measures of surveillance – and, in particular, the interception of communications – apply to the regime permitting the bulk interception and processing of communications and related communications data?"*

25. The Applicant submits that there are compelling reasons why modern bulk interception regimes should be considered as inherently incompatible with the Convention. If the Court, nevertheless, considers that the decision to operate a bulk interception regime falls within the States' margin of appreciation, it is imperative that the Court sets down robust minimum safeguards.

26. In setting down these standards, the Applicant submits that the factors outlined in *Roman Zakharov* as listed in paragraph 23 above serve as an appropriate initial framework. However, the elevated privacy risks caused by rapid technological developments and the differences in the nature and scope of untargeted surveillance require these standards to be adapted and updated to be appropriate.[20]

[19] *Roman Zakharov*, cited above, § 238.

[20] *Cf.* Partly Concurring, Partly Dissenting Opinion of Judge Koskelo in *Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13 and 2 others, § 19, 13 September 2018.

2.3.1 There are compelling reasons why modern bulk interception regimes should be considered as inherently incompatible with Article 8 of the Convention.

(i) Lack of proportionality

27. The Court has consistently considered the targeted nature of a surveillance regime as a relevant consideration in deeming it compatible with the Convention. In *Klass v. Germany*, the Court even explicitly attached weight to the fact that the contested regime did not permit "so-called exploratory or general surveillance".[21] In *Association "21 December 1989" and Others v. Romania*, the Court found a violation in part because the purpose of the surveillance measures had been exploratory general surveillance.[22]

28. When the Court has deemed untargeted interception regimes compatible with the Convention, these have been far more confined in scope than the Swedish system. In *Weber*, less than 10% of all telecommunications could be monitored. The strategic monitoring did not cover internet communications and the identity of the person could rarely be ascertained.[23] In *Liberty*, the untargeted surveillance activities were confined to telecommunications channels between England and Ireland.[24]

29. By contrast, the Swedish signals intelligence agency, the National Defence Radio Establishment (*Försvarets radioanstalt*, the "**FRA**") can gain access to virtually all cable-based communications crossing the Swedish border.[25] Due to the global nature of the infrastructure of the internet and the ever increasing extent to which we live our lives online, the amount of intimate, private and privileged data that can now be surveyed under the Swedish signals intelligence regime, is far greater than under any other regime reviewed by the Court – save for the regime currently under review in *Big Brother Watch*. Therefore, the proportionality calculation is entirely different in the present Case.

30. The Applicant acknowledges the need to intercept communications as part of concerted efforts to counter threats to national security. To that end, it is reasonable that targeted interception regimes and even smaller-scale untargeted interception regime may fall

[21] *Klass and Others*, cited above, § 51.

[22] *Association "21 December 1989" and Others* v. Romania, nos. 33810/07 and 18817/08, §§ 174–175, 24 May 2011.

[23] *Weber and Saravia*, cited above, § 110.

[24] *Liberty and Others,* cited above, § 5.

[25] Chamber Judgment, § 94.

within the States' margin of appreciation. Nonetheless, it may very well be the case that the technological capacities of governments to spy on its citizens are now far exceeding the limits of what can be acceptable in a democratic society governed by the rule of law.

(ii) Lack of consistency with other areas of the Convention's case law

31. Signals intelligence cannot be considered compatible with the Convention solely on account of its purported utility in identifying previously unknown threats to national security. This is the case, the Applicant submits, even if certain safeguards are in place.

32. Indeed, in a line of case law relating to systematic gathering of personal data, the Court has repeatedly held that utility is not in itself a sufficient basis for justifying an interference. For instance, in *S and Marper v. the United Kingdom*, the Grand Chamber found that blanket retention of fingerprints, cellular samples and DNA profiles of persons suspected, but not convicted, of offences fell outside any acceptable margin of appreciation.[26] This was so notwithstanding the fact that the Government considered such retention "indispensable in the fight against crime".[27] A similar conclusion was reached by the Court in *M.K. v. France*.[28]

33. Holding that large-scale modern bulk interception regime fall within the margin of appreciation afforded to Contracting States risks leading to an inconsistent application of the Convention. This would be contrary to the principle that the Convention must be read as a whole, and interpreted as to promote internal consistency and harmony.[29]

34. The Court may, notwithstanding these considerations, nevertheless decide that operating a bulk interception regime of the intensity and scale as the Swedish signals intelligence regime falls within the margin of appreciation afforded to Contracting States. In doing so, the Court will send a clear statement to the rest of Europe that the Convention permits its governments to intercept and analyse, in secret, enormous quantities of private communications and personal information of citizens and organisations who are not

[26] *S. and Marper*, cited above, § 125.

[27] *S. and Marper,* cited above, § 115.

[28] *M.K. v. France*, no. 19522/09, § 46, 18 April 2013.

[29] See *inter alia Stec and Others v. the United Kingdom* (dec.) [GC], nos. 65731/01 and 65900/01, § 48, ECHR 2005-X.

suspected of a crime, are not themselves suspected of constituting a threat to national security, and the great majority of whom are of no intelligence interest at all.

35. If the Court is prepared to do so, it must not hesitate in setting down robust minimum safeguards. These must be appropriately formulated, and, where necessary, updated to address the distinct privacy risks and technical realities of a modern bulk interception regime. If bulk interception truly falls within the margin of appreciation, it inevitably lies on its outermost edge. It must be restricted accordingly.

2.3.2 To the extent that modern bulk interception regimes are capable of falling within the margin of appreciation, they must contain adequate and effective safeguards, appropriately adapted

(iii) The main elements of the bulk interception regime should be set out in sufficient detail in statute law

36. Firstly, the Court is invited to hold that the main elements of the surveillance regime must be set out in sufficient detail in statute law.

37. The purpose of defining secret surveillance powers with sufficient precision is to reduce the scope for abuse. Especially where a power vested in the executive is exercised in secret, the risk of arbitrariness is evident. Thus, in a field where abuse is potentially easy in individual cases, and could have harmful consequences, constraining the powers of the executive only through secondary legislation or case law is not sufficient.

38. The Applicant submits that it should be for the representatives of the people to make the decision to institute a bulk interception regime and, through setting out its main elements, strike the necessary balance between competing interests in an area as important as this. Statutory regulations are also more stable and transparent than regulation by means of subordinate legislation or case law.[30]

39. In conclusion, the Applicant submits that the main elements of a secret bulk surveillance regime must be set out in statute law in order to ensure that the legislative branch is

[30] See on this point CDL-AD(2015)011-e, *Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session* [Venice, 20–21 March 2015], ("**Venice Commission Report 2015**"), para. 93 (Enclosure 1).

involved in the balancing between different interests and to promote foreseeability, transparency and public trust in this important area.

(iv) There should be a requirement of effective prior judicial authorisation

40. Secondly, the Grand Chamber should, in the Applicant's submission, take this opportunity to affirm the centrality of judicial oversight by making it a necessary requirement under the Convention.

41. It follows from the Court's existing case law that the authority competent to authorise the surveillance may be a non-judicial authority, as long as that authority is sufficiently independent from the executive.[31] Thus, the Court has not yet set a requirement for prior judicial authorisation. The Applicant submits that due to present-day realities of far-reaching surveillance techniques and prerogatives, the time has come to do so.

42. The Court has repeatedly held that it is desirable to entrust supervisory control to a judge in the domain of interception activities, as it offers the best guarantees of independence, impartiality, and proper procedure. This is particularly important in the field of secret surveillance, where the potential for abuse and the potential harm for individuals and the wider democratic society are so great.[32]

43. In *Big Brother Watch*, the Court regrettably did not find that prior authorisation had to be judicial. As Judge Koskelo noted in her separate opinion, the main argument against doing so seemed to be that judicial scrutiny may fail its function and would thus, by itself, not be sufficient to ensure compliance with Article 8.[33]

44. The Applicant concurs with Judge Koskelo, that the fact that prior judicial authorisation might not be sufficient in itself to protect against abuse, does not support the conclusion that it should not be considered necessary under the Convention. Quite the contrary, the notion that even judicial scrutiny may fail its function further underscores the need for prior authorisation by a judge, which offers the best guarantee of independence.[34]

---

[31] See *Roman Zakharov*, cited above, § 258; and *Dumitru Popescu v. Romania* (no. 2), no. 71525/01, § 71, 26 April 2007.

[32] See *Roman Zakharov*, cited above, § 233; and *Klass and Others,* cited above, §§ 55–56.

[33] *Big Brother Watch and Others*, cited above, §§ 319–320; and Judge Koskelo in *Big Brother Watch and Others*, cited above, § 25.

[34] Judge Koskelo in *Big Brother Watch and Others*, cited above, §§ 25–28.

45. The European Commission for Democracy through Law (the "**Venice Commission**") has emphatically held that external oversight needs to be considerably strengthened in the field of signals intelligence.[35] Arguably, if authorising surveillance is left to the executive branch, there is a great risk of it over-collecting intelligence and discounting individual rights. The executive cannot sufficiently check itself in this context.

46. The Court should, therefore, in the Applicant's submission, take this opportunity to affirm the centrality of judicial oversight to the minimum safeguards for individual rights and freedoms by making it a necessary requirement under the Convention.[36]

47. Of further relevance is the scope of review and the necessary contents of the warrant to conduct secret surveillance. The Court has had regard to the scope of review and the content of the interception warrant in assessing whether the authorisation procedures are capable of ensuring that secret surveillance is not conducted haphazardly, irregularly, or without due and proper consideration.[37] The prior authorisation should, in other words, not only be judicial, but also effective. To that end, some further strengthening of the applicable standards is required in terms of the relevant scope of review.

(v) The authorising body should be capable of verifying that individuals are only subjected to, or implicated in, bulk interception activities on the basis of reasonable suspicion or an appropriate materiality threshold

48. Thirdly, the Court should require that the body authorising the surveillance be capable of verifying the existence of reasonable suspicion in relation to any person the Government seeks to single out and target in the context of the bulk interception activities. In case there are no predefined targets, the Court should instead require that the authorising body be capable of verifying that personal data is only used as search terms[38] to the extent that such data is material to a narrowly specified foreign intelligence objective. In other words, the personal data should reach a certain materiality or relevance threshold.

---

[35] Venice Commission Report 2015, paras. 21 and 105 (Enclosure 1).

[36] As Judge Koskelo also contends, see Judge Koskelo in *Big Brother Watch and Others*, cited above, § 29.

[37] See *Roman Zakharov*, cited above, § 257.

[38] The Swedish legislation specifically uses "search terms" to refer to terms employed in the process of collecting signals. For the sake of simplicity, the Applicant will use "search terms" also to refer to the terms used to search the bulk collected data in the subsequent processes of minimisation and analysis.

49. The Applicant submits that even if the authorising body is judicial, as under the Swedish regime, it is not an effective control mechanisms unless it can verify materiality of personal data being used as search terms, or, where appropriate, reasonable suspicion. The Applicant will deal first with materiality and then with reasonable suspicion.

50. In the Applicant's submission, the use of search terms relating to a specific individual exposes that individual to distinct privacy risks. The automated processing of personal data is inevitably associated with a risk of misuse and abuse, especially if it to some extent is done in secret. Use of search terms relating to specific individuals will also, more specifically, risk disclosing sensitive and intimate information relation to their conduct, opinions or feelings. Such use should, therefore, only be permitted in so far as the data is material to a narrowly specified foreign intelligence objective.

51. As for reasonable suspicion, the Court held in *Roman Zakharov* that communications may only be intercepted where the body authorizing the surveillance has confirmed that there is a "reasonable suspicion" of wrongdoing on the part of the persons concerned.[39]

52. The Chamber in the present case appears to have implicitly excluded the reasonable suspicion requirement from the prior authorisation measures set out in *Roman Zakharov* altogether – without any justification for doing so. This represents either a deliberate departure from the Grand Chamber's established jurisprudence in *Roman Zakharov*, or an unreasoned distinction made between cases of targeted and bulk interception, or between law enforcement and foreign intelligence.

53. In *Big Brother Watch*, the Court also dispensed with the requirements in *Roman Zakharov* to require reasonable suspicion against a targeted individual. The Court stated that "bulk interception is by definition untargeted, and to require 'reasonable suspicion' would render the operation of such a scheme impossible".[40]

54. Respectfully, this reasoning fails to consider that individuals may nevertheless be targeted or be implicated in bulk interception activities through the use of personalised search terms. This is illustrated by the fact that the Swedish signals intelligence regime expressly permits the use of such search terms.[41] As mentioned above, the use of search terms directly relating to a specific individual has serious privacy implications. This is

[39] See *Roman Zakharov*, cited above, § 260. See also *Szabó and Vissy*, cited above, § 71.

[40] *Big Brother Watch and Others*, cited above, §§ 316 and 317.

[41] Chamber Judgment, § 16.

particularly the case if they are used to single out and gather data on a particular individual in order to profile intimate detail of that individuals private life.

55. Failing to apply the same threshold for use as applies to targeted interception risks creating a dangerous lacuna in the protection afforded by the Convention, and opens up the possibility for personalised bulk interception searches being used as a work-around method for targeting individuals.

56. The Applicant consequently submits that in order to be deemed sufficiently effective, the authorising body should be capable of verifying the existence of reasonable suspicion, where personalised search terms are used in order to single out or target specific individuals as part of a broader bulk interception activity. Where there are no clearly defined surveillance targets, a materiality threshold should apply instead.

(vi) The authorising body should be capable of reviewing not only the interception but also the intended subsequent use

57. Fourthly, the Court is invited to hold that the authorising body must be capable of reviewing the intended use of collected data. For that purpose, the signals intelligence agency should be required to provide an indication of how the data will be analysed in its request for a warrant.

58. Such an indication should include whether analysts intend to conduct pattern-based or subject-based data mining, whether profiles on individuals will be compiled and whether the data will be subject to complex and comprehensive analysis by computer, and in such case to what end.

59. The Applicant submits that a requirement of this kind would considerably fortify prior judicial authorisation as a mechanism for ensuring that any interference is kept to what is "necessary in a democratic society."

(vii) Effective supervision and remedies should be affirmed as forming part of the minimum safeguards

60. Lastly, the Court is invited to affirm that effective supervision and effective remedies do form part of the minimum safeguards.

61. In *Roman Zakharov*, the Court identified supervision, notification and remedies as "additional relevant factors" but did not classify them as "minimum requirements".[42] The Applicant submits that bulk interception can only be deemed necessary in a democratic society if there is effective supervision in place to minimise the risk of abuse and effective remedies that can afford individuals appropriate redress. In this connection, notification is closely linked to the effectiveness of the remedies. See further section 2.4.9 below

62. Accordingly, the Applicant submits that the Court, to the extent they are not already considered as such, should take this opportunity to establish that effective supervisory and remedial mechanisms form part of the necessary minimum safeguards.

(viii) Specific requirements relating to supervision and remedies

63. Question 2c of the Court's Questions states:

> *"Does Article 8 § 2 also require supervision and review of the impugned activities by an independent body and, if so, what level of independence from the Government is needed? In view of the specific type of analysis in bulk interception, at what stage(s) would it be appropriate for supervision to take place? What type of supervision and review, if any, is required when the surveillance is first ordered, while it is being carried out, and after it has been terminated? Should there be a body entrusted with oversight powers which is capable of rendering legally binding decisions? If so, at what stage(s)?*

64. As the Court indicates, review and supervision of secret surveillance 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.[43] In section 2.3.2 (iv) above, the Applicant has submitted that review carried out when the surveillance is first ordered, *i.e.* at the first stage, should be carried out by a judicial body. In the following subsections, the Applicant will address the Court's Questions on supervision and review in relation to the second and third stages.

(ix) Supervision and review by an independent body is required

65. It follows from the Court's established case law that supervision and review of the implementation of the secret surveillance measures must be performed by an independent body.[44] If effective external oversight mechanisms are not in place the "procedures for

[42] See *inter alia Big Brother Watch and Others,* cited above, § 320; and *Roman Zakharov*, cited above, § 238.

[43] *Cf. Roman Zakharov*, cited above, § 233.

[44] See *inter alia Roman Zakharov,* cited above, § 275; and *Klass and Others*, cited above, § 56. See also Venice Commission Report 2015, para. 105 (Enclosure 1).

supervising and ordering the implementation of the restrictive measures" can hardly be capable of keeping the "interference" to what is "necessary in a democratic society".[45]

(x) The level of independence required

66. To assess whether the supervising body is sufficiently independent, regard must be had to the manner of appointment and the legal status of the members of the oversight body, as well as any potential conflicts of interest. In particular, the Court has found sufficiently independent oversight bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office.[46] The Applicant submits that the main oversight *ex post* should be carried out by an oversight body that reaches this particular level of independence from the executive branch. As will be further detailed below, the Applicant is satisfied that Swedish oversight bodies meet the requirement of sufficient independence.

(xi) The type of supervision and review required at different stages

67. In accordance with the Court's established case law, the Applicant submits that an oversight body must be capable of ensuring that the statutory requirements relating to the implementation of secret surveillance measures, storage, access to, processing, communication, and destruction of intercepted material are respected.[47]

68. In view of the specific type of analysis in bulk interception, supervision should appropriately focus on the three key stages of data processing. The first of those key stages is when the collected communications are subject to automated computer analysis with the help of search terms to filter out irrelevant data.[48] The second key stage is where human analysts undertakes further minimisation, data mining, and analysis.[49] The third key stage is the communication of data or finalised intelligence reports to other national authorities, foreign Governments or international organisations. Storage of data at each stage should also be subject to particular supervision and review.

---

[45] *Cf. Roman Zakharov,* cited above, §§ 232.

[46] *Roman Zakharov,* cited above, §§ 278–280.

[47] *Roman Zakharov,* cited above, § 273.

[48] See Venice Commission Report 2015, para 42 (Enclosure 1).

[49] *Cf.* Venice Commission Report 2015, para 44 (Enclosure 1).

69. To carry out this review, the oversight bodies must be "vested with sufficient powers and competence to exercise an effective and continuous control".[50] They should be capable of taking measures to stop or remedy any detected breaches of law and bring those responsible to liability. Their activities should be open to public scrutiny.[51] They should also have access to classified documents.[52] In this connection, the Court has consistently held that an obligation on the intercepting agencies to keep records of interceptions is particularly important to ensure that the supervisory body has effective access to details of the surveillance that has been carried out.[53]

70. Finally, it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples.[54]

(xii) Effective remedial mechanisms must be in place

71. As for the third stage referred to above, the existence of effective safeguards against the abuse of monitoring powers is inextricably linked to the effectiveness of individual remedies before the courts. The effectiveness of the remedies are in turn inextricably linked to the possibility for individuals to be advised of the surveillance measures carried out without their knowledge.[55]

72. It thus follows from the Court's case law that the effectiveness of remedies in the secret surveillance context can rely on either:

    a) the subject of surveillance being notified of the surveillance after it has been concluded,
    b) there being an effective possibility to request and obtain information about the surveillance from the authorities, or

[50] *Roman Zakharov*, cited above, § 275; and *Klass and Others*, cited above, § 56.

[51] *Roman Zakharov*, cited above, §§ 282–284.

[52] See European Union Agency for Fundamental Rights, 2017, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: Field perspectives and legal update*, p. 114 (Enclosure 2).

[53] See *inter alia Roman Zakharov*, cited above, § 272; and *Kennedy*, cited above, § 165.

[54] *Roman Zakharov*, cited above, § 284.

[55] See *Roman Zakharov*, cited above, § 234.

c) there being a body that can effectively examine individual complaints without any requirement on the individual to produce evidence.[56]

73. To be effective, a remedial body must, furthermore, have access to classified information and be capable of affording appropriate redress.[57]

(xiii) Both oversight and remedial bodies should be capable of rendering legally binding decisions

74. The Applicant submits that both oversight bodies and remedial bodies must be capable of rendering legally binding decisions in order to be considered effective.

75. As the Court held in *Roman Zakharov*, the oversight body should be capable of taking measures to stop or remedy any detected breaches of law and to bring those responsible to liability.[58] This presupposes, in the Applicant's submission, that the oversight body has the power to render legally binding decisions.

76. Moreover, as pointed out above, a remedial body must be capable of affording appropriate redress in order to be considered effective, which in most cases require the power to issue binding decisions. The EU Fundamental Rights Agency has specifically emphasised that the effectiveness of remedies depends on the capacity to issue legally binding decisions, which at a minimum should include the ability to order termination of the surveillance, destruction of collected data, and payment of appropriate compensation.[59]

77. For these reasons, the Court is invited to confirm that oversight and remedial bodies alike must be capable of rendering legally binding decisions to be deemed effective.

(xiv) Content and related communications data must be subject to the same safeguards

78. Question 2d of the Court's Questions states:

"*Should the same principles apply to both content and related communications data?*"

---

[56] See *Roman Zakharov*, cited above, §§ 234, 291 and 298; and *Kennedy*, cited above, § 167.

[57] See *inter alia Šantare and Labazņikovs v. Latvia*, no. 34148/07, §§ 60–62, 31 March 2016 on access to information; and *Tomov and Others v. Russia*, no. 18255/10 and 5 others, §§ 148 and 194, 9 April 2019 on binding decisions.

[58] *Roman Zakharov*, cited above, §§ 282–284.

[59] See European Union Agency for Fundamental Rights, 2017, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: Field perspectives and legal update*, p. 114 (Enclosure 2).

79. In view of technological developments, collection of communications data now constitutes an even greater intrusion, and involves even greater risks of abuse, than collection of communications content.[60] For that reason, it is vital that the same principles apply to both communications content and related communications data.

80. In any event, different safeguards and standards cannot apply in the present case as the legal framework governing the Swedish signals intelligence regime does not differentiate between content and related communications data.

2.4 Application of the Convention standards to the present Case

2.4.1 Basis in law and legitimate aim

81. The Applicant does not dispute that the Swedish signals intelligence regime has a formal basis in statutory law and is carried out in pursuit of a legitimate aim.

82. The Applicant's previous submissions made references to three distinct time periods since 2008 in the Swedish signals intelligence regime. The following sections focus only on the Swedish legislation as it stands as of 3 May 2019.[61]

2.4.2 Accessibility of domestic law

83. The Applicant does not dispute that all relevant legal provisions have been officially published and are accessible to the public.[62]

2.4.3 Scope of application of signals intelligence

84. The Applicant concedes that the general scope of application of the FRA's signals intelligence powers under the current legislation is sufficiently constrained. The development activities of the FRA, which grants a wide discretion to intercept communications without a clear connection to specific national security threats, are, however, still cause for concern.[63]

---

[60] See, *e.g.*, Judgment of 21 December 2016, Joined Cases *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, ECLI:EU:C2016:970, § 99 (Enclosure 3); see also Advocate General Henrik Saugmandsgaard Øe's Opinion, § 259 (Enclosure 4).

[61] *Cf.* Chamber Judgment, §§ 96–98.

[62] See Chamber Judgment, § 115.

[63] *Cf.* Chamber Judgment, § 122.

85. It is also concerning that the Security Police and the National Operative Department of the Police Authority (the "**NOA**") since 1 January 2013 have been empowered to issue tasking directives for signals intelligence, and that as of 1 March 2018, the Security Police may be granted direct access to FRA's databases with analysis material.

86. Furthermore, the Government has recently introduced a proposed bill, which will enable the Security Police and the NOA to gain direct access to data collected through signals intelligence even in relation to events subject to an ongoing criminal investigation. The proposal was introduced to the Parliament on 11 April 2019, and the new rules are proposed to enter into force on 1 August 2019.

87. Even though there are provisions prohibiting the use of foreign intelligence to solve tasks relating to law enforcement,[64] the increasing powers for law enforcement agencies to commission signals intelligence and access collected data or intelligence reports, raises doubts as to conformity with the finality principle, *i.e.* that personal data must be collected and processed only for specific, explicit legitimate purposes, and may not be used in a way that is inconsistent with those purposes.[65] In the legislative consultation process for the proposal currently before Parliament, the Foreign Intelligence Inspectorate (*Statens inspektion för underrättelseverksamheten*, SIUN, the "**Inspectorate**"), the main oversight body, raised concerns that the law enforcement agencies would not bee able to keep information received from the FRA separate from their law enforcement activities.[66]

88. It is critical that the risk of signals intelligence being used outside the scope of foreign intelligence activities is sufficiently contained by clear legal provisions and effective supervision and review. The Applicant respectfully asks the Court to take this into account in its overall assessment of the lawfulness and necessity of the Swedish regime.

2.4.4 Limits on the duration of secret surveillance measures

89. 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

[64] See Chamber Judgment, § 123.

[65] See, *e.g.*, Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, CETS No.108, Articles 5(b) and (e) (Enclosure 5).

[66] Comments by the Inspectorate on legislative proposal DS 2018:35, 15 November 2018 (Enclosure 6).

expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled.[67]

90. The Swedish Signals Intelligence Act requires warrants to have a clear expiry date and sets out the conditions for renewal. However, there is no requirement that a warrant must be cancelled if collection of communication under the warrant ceases to be necessary.[68] Swedish law thus satisfies the first two cumulative safeguards laid down in *Roman Zakharov*, but fails the third.[69] For that reason, the Applicant submits that the Swedish signals intelligence regime does not meet the required standards in this regard.

2.4.5 Prior judicial authorisation

91. The Applicant is satisfied that the authorising body, the Foreign Intelligence Court (*Försvarsunderrättelsedomstolen*), is a judicial body and thus meet the updated requirement relating to prior judicial authorisation proposed in section 2.3.2 (iv) above. The scope of the judicial review afforded by the Foreign Intelligence Court is, however, too limited to be effective.

92. Firstly, the Foreign Intelligence Court is not required to verify the existence of reasonable suspicion in relation to any person the Government seeks to single out and target in the context of the bulk interception activities.

93. Secondly, the applicable materiality threshold only applies to search terms being use for the collection of data. Under the Signals Intelligence Act, search terms relating directly to a specific natural person may be used if it is of "exceptional importance" to the intelligence activities.[70] However, this provision only refers to terms employed in the automated collection of data and not to the search terms used to search the bulk collected data.[71] The Foreign Intelligence Court can thus not verify the materiality of the personal data the FRA employs as search terms after the initial collection.

94. Thirdly, the Foreign Intelligence Court is not required to review the intended subsequent use of the collected data. The FRA is under no obligation to provide in its warrant request

---

[67] See *Roman Zakharov*, cited above, § 250.

[68] Section 5a of the Signals Intelligence Act (*Lagen om signalspaning i försvarsunderrättelseverksamhet;* 2008:717) (Enclosure 7).

[69] As the Chamber also concluded, see Chamber Judgment, § 129.

[70] Section 3 of the Signals Intelligence Act (Enclosure 7).

[71] *Cf.* Venice Commission Report 2015, p. 9 footnote 8 (Enclosure 1).

any indications of how the data will be analysed, such as whether analysts intend to conduct subject-based data mining, whether profiles on individuals will be compiled and whether the data will be subject to complex and comprehensive analysis by computer, and in such case to what end. The Swedish regime, therefore, fails to satisfy the proposed updated safeguard on prior authorisation of intended use.

95. In sum, the authorisation procedure does not meet the updated requirements under the Convention that the Court has been invited to lay down (see section 2.3.2 (vi) above).

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

96. The Applicant concedes that though the procedures to be followed for storing, accessing, examining, using and destroying the intercepted data are regulated in broad terms, the legislation is largely sufficient in this respect.[72] There are, however, two major flaws.

97. Firstly, there is no explicit legal obligation on the FRA to keep detailed records of interception, subsequent use and communication of data. The Swedish Data Protection Authority (*Datainspektionen*) has repeatedly criticised the FRA for not adequately keeping logs. Although this issue was pointed out by the Data Protection Authority in 2010, the FRA had still not addressed it in 2016.[73] This shortcoming hinders effective review by the oversight bodies.

98. Secondly, the storing, accessing, examining, using, and destroying of intercepted data is almost exclusively governed by the FRA Personal Data Processing Act (*Lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet; 2007:259*) (Enclosure 8). That act was adopted before the Signals Intelligence Act and, as the Data Protection Authority has held, has not been adapted to fit the bulk interception context.[74]

---

[72] See Chamber judgment, § 142.

[73] Report of the Data Protection Authority, 24 October 2016, *Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, p. 1 (Enclosure 9). See also Report of the Data Protection Authority, 6 December 2010, *Datainspektionens redovisning av regeringsuppdraget,* Fö 2009/355/SUND, p. 4 (Enclosure 10).

[74] Report of the Data Protection Authority, 24 October 2016, *Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, pp. 18–19 (Enclosure 9).

2.4.7 Conditions for communicating data to other parties

99. The Applicant concedes that the conditions for communicating data to other national authorities are sufficiently circumscribed. As mentioned above in relation to the scope of application of signals intelligence, the Court is, nonetheless, asked to take into consideration that communication of foreign intelligence, which may not be used for law enforcement or crime prevention, to law enforcement agencies raises doubts as to conformity with the finality principle.

100. In order to respond fully to the Court's Questions in regard to communication of data to foreign third parties, that issue will be dealt with separately under section C below.

2.4.8 Supervision

101. The Applicant concedes that the supervisory elements of the Swedish signals intelligence regime satisfy most of the requirements of the Convention. Still, it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples.[75] The Applicant submits that the supervision is not sufficiently effective and that the Government has not been able to demonstrate the opposite.

102. Crucially, the Swedish system fails to fully afford the oversight bodies the power to "stop or remedy the detected breaches of law and to bring those responsible to liability".[76] To that end, the oversight bodies must, as the Applicant has submitted above, have the power to render legally binding decisions. The only body capable of doing so is the Inspectorate, and even the Inspectorate can only render legally binding decisions to a limited extent.

103. The Inspectorate may decide that a particular signals intelligence operation shall cease or that the intelligence shall be destroyed, if it finds that the operation is incompatible with a warrant granted by the Foreign Intelligence Court.[77] However, the Inspectorate does not have the power to review or quash a warrant that is deemed unlawful.[78] As long as the operations are compatible with a warrant, the Inspectorate has no power to issue binding decisions. That holds true even if the Inspectorate finds that the operations are unlawful on other grounds, for instance, if it violates data protection provisions, the Swedish

[75] See *inter alia Roman Zakharov*, cited above, § 284.

[76] See *inter alia Roman Zakharov*, cited above, § 282.

[77] Section 10 of the Signals Intelligence Act.

[78] Preparatory works prop. 2008/09:201, p. 114 (Enclosure 11).

Constitution or the Convention. Under no circumstances does the Inspectorate have the power to grant compensation to individuals or to bring those responsible for any breaches of the law to liability. The powers of the Inspectorate to render legally binding decisions is, therefore, too limited to be sufficiently effective.

104. The Data Protection Authority, which supervises the FRA's compliance with the FRA Personal Data Processing Act and complements the review carried out by the Inspectorate in that respect, does not have the power to issue any legally binding decisions in relation to the FRA. If the Data Protection 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.[79] It may also apply to the Administrative Court in Stockholm (*Förvaltningsrätten i Stockholm*) to have illegally processed personal data destroyed.[80]

105. The Chancellor of Justice (the "**Chancellor**") and the Parliamentary Ombudsmen (the "**Ombudsmen**"), whose general oversight functions the Government has referred to, may not issue legally binding decisions either. They are tasked with examining whether courts and authorities in general comply with laws and regulations and fulfil their obligations. As the Court noted in *Segerstedt-Wiberg and Others v. Sweden*, the Chancellor and the Ombudsmen do not have any specific responsibilities to supervise secret surveillance.[81]

106. To this date, neither the Chancellor nor the Ombudsmen have carried out any inspections of the FRA on their own initiatives. As of 8 April 2019, the Chancellor had received 12 complaints from individuals relating to the FRA. All complaints were dismissed without any action taken.[82] As of 5 April 2019, the Ombudsmen has received 13 complaints from individuals. All complaints were dismissed with no action taken, save for in one case where the Ombudsmen made a single phone call to the FRA.

107. The fact that the Chancellor and the Ombudsmen does not have any specific responsibilities to oversee the FRA, and given the complex nature of its operations, it is highly unlikely that those bodies possess the necessary knowledge in order to carry out inspections of the FRA's operations effectively and adequately. Furthermore, in the

[79] Chapter 5, section 3 of the FRA Personal Data Processing Act (Enclosure 8).

[80] Chapter 5, section 4 of the FRA Personal Data Processing Act (Enclosure 8).

[81] *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 118, ECHR 2006-VII.

[82] See letter from the Chancellor dated on 8 April 2019 (Enclosure 12).

Ombudsmen's own admission, in view of its function as an "extraordinary oversight body", it is not unlikely that the Ombudsmen will refrain from investigating individual complaints against the FRA due to the fact that the primary responsibility to oversee the FRA is tasked to the Inspectorate.[83]

108. To conclude, the Applicant submits that the supervisory arrangements in the Swedish signals intelligence regime are not sufficiently effective. The Government has not been able to illustrate the practical effectiveness of the supervision arrangements with appropriate examples. Therefore, the supervisory arrangements cannot be considered capable of keeping the interference to what is "necessary in a democratic society."

2.4.9 Remedies

109. The Applicant further submits that the Swedish signals intelligence regime fails to provide individuals with proper recourse to adequate and effective remedies for unlawful or improper surveillance.

(i) The provision of adequate and effective remedies is a crucial safeguard against abuse.

110. The Court has repeatedly emphasised in its case law on secret surveillance the importance of adequate and effective remedies for individuals and organisations against unlawful or improper surveillance.[84] Sufficient recourse to such remedies is vital to ensure that interference caused by secret surveillance is kept to what is necessary in a democratic society. Judge Pinto de Albuquerque has even referred to the access to remedy as "the most important safeguard against [the] improper use of secret surveillance measures".[85]

(ii) The notification requirement under Swedish law lacks practical significance.

111. Under section 11(a) of the Signals Intelligence Act, the FRA must notify an individual when search terms directly related to them have been used as part of an interception activity. However, this obligation may be disapplied if required for reasons of secrecy. The Applicant submits that this remedy is both deficient and "theoretical and illusory" in

[83] See email from the Ombudsmen dated on 5 April 2019 (Enclosure 13).

[84] See *inter alia Roman Zakharov,* cited above, § 234 and *Weber and Saravia*, cited above, § 135.

[85] Separate Opinion of Judge Pinto de Albuquerque, *Szabó and Vissy*, cited above, § 34.

effect.[86] It is deficient as it only pertains to natural persons, and is therefore not available to organisations such as the Applicant. It is "theoretical and illusory" in effect as notification is invariably withheld due to secrecy. The Government has confirmed that the FRA has never once issued a notification to an individual,[87] which lead to the Chamber agreeing with the Applicant that the notification requirement "lacks practical significance".[88]

112. The Applicant is cognisant that the subsequent notification of individuals that have been subject to interception is not always feasible in the secret surveillance context, as doing so may compromise the efficacy of the surveillance operation.[89]

(iii) Effective remedies may nevertheless be provided without the requirement for notification.

113. The Applicant submits, however, that despite the challenges in providing practical and effective remedies within the secret surveillance context, the State must nevertheless provide remedies that are "as effective as can be" in the context.[90]

114. It is possible to do so without the need for notification. The Court affirmed this view in *Kennedy* and *Big Brother Watch*, where it found that the Investigatory Powers Tribunal ("**IPT**") in the United Kingdom gave individuals sufficient recourse to a remedy. The Court highlighted that the IPT – an independent and impartial tribunal with judicial qualities – had jurisdiction to hear individual complaints of unlawful interception without the need for such individuals to prove that they had been subject to surveillance. The IPT had access to all relevant secret documents. It had the ability to quash interception orders, could order the destruction of intercepted material, and crucially, had the power to order the payment of compensation to victims. Its legal rulings were also published, which

[86] Chamber Judgment, § 166.

[87] Chamber Judgment, § 163.

[88] Chamber Judgment, § 165.

[89] *Roman Zakharov*, cited above, § 287.

[90] See *inter alia Klass and Others,* cited above, § 69; *Leander,* cited above, § 78; *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 99; and *mutatis mutandis*, *Chahal v. the United Kingdom*, 15 November 1996, § 150, *Reports of Judgments and Decisions* 1996-V.

enhanced the level of scrutiny it provided.[91] No such arrangements, or their equivalent, exist in Sweden.

(iv) The Government has, however, failed to demonstrate that the remedies available under Swedish law are effective

115. It is for the Government to establish not only the existence of an adequate remedy, but its practical effectiveness.[92] The Applicant submits that the Government has failed to demonstrate that the limited remedial channels available under Swedish law are effective in the absence of any possibility for the individual to be informed of surveillance taking place. The following subsections examine each of them in turn.

(v) Individual request for review by the Inspectorate is not an effective remedy

116. An individual may submit a request asking the Inspectorate to investigate if their communications have been intercepted through signals intelligence and, if so, to verify whether the interception and treatment of the information have been in accordance with the law. The Inspectorate shall, however, only notify the individual that such an investigation has been carried out and need not inform the individual of its findings.[93]

117. Furthermore, as has been noted above, the Inspectorate has the power to order that a particular signals intelligence operation shall cease or that the intelligence shall be destroyed only if it finds that an operation violates a warrant. Thus, the Inspectorate cannot order the FRA to cease an operation on the basis that the surveillance violates the Signals Intelligence Act, the FRA Personal Data Processing Act, the Swedish Constitution, or the Convention.[94]

118. Moreover, as the Chamber observed, the Inspectorate may not order the payment of compensation. However, the Chamber went on to state that it was "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".[95] Respectfully, the Applicant submits

[91] *Kennedy*, cited above, § 167. See also *Big Brother Watch and Others*, cited above, § 379.

[92] See, *e.g.*, *Roman Zakharov,* cited above, § 295.

[93] Section 10a of the Signals Intelligence Act (Enclosure 7).

[94] Chamber Judgment, § 171.

[95] Chamber Judgment, § 172.

that the Chamber erred in its assessment, and has unfortunately overestimated the effectiveness of these remedies.

(vi) The Chancellor of Justice is not an effective remedy in this context

119. The Chancellor may award compensation in response to certain claims from an individual for wrongdoing by the Government. This power of the Chancellor is laid down in the Ordinance concerning the administration of claims for damages against the Government (*förordningen om handläggning av skadeståndsanspråk mot staten;* 1995:1301) (Enclosure 14). A decision by the Chancellor to reject an individual's claim for damages is not subject to appeal. The Applicant submits that seeking compensation from the Chancellor is not effective for the following three reasons.

120. Firstly, the Chancellor only awards compensation in cases where it is evident that an individual is entitled to compensation from the Government. It is the individual who has the burden of proof to establish that all necessary elements of liability for damages are satisfied. Without any evidence of unlawful surveillance, an individual is unlikely to be able to establish that their right to compensation is evident.

121. Secondly, a right to compensation might not in itself be sufficient to afford appropriate redress. In *Segerstedt-Wiberg*, the possibility to seek compensation did not offset the fact that the applicants had no access to any legal remedies through which they could obtain erasure of unlawfully processed data.[96] The same is true in the present case.

122. Thirdly, it is unlikely that the Chancellor will take, or even be able to take, any meaningful action in response to any unlawful activities of the FRA. Whilst the Chancellor has a general duty to investigate complaints received by the public, under section 15(2) of the Ordinance with Instruction for the Chancellor of Justice, the Chancellor is afforded a wide discretion to determine precisely which complaints to review. The Chancellor's approach until the present day has hardly demonstrated an attentiveness to the privacy concerns arising from large-scale surveillance. As of the date of these submission, the Chancellor has dismissed all complaints against the FRA and has taken no related action.[97]

123. Moreover, there is a possibility that the Chancellor may be informed of incidents at the FRA that may incur liability for damages for the Government. If the Inspectorate

[96] *Segerstedt-Wiberg and Others,* cited above, § 121.

[97] See letter from the Chancellor dated on 8 April 2019 (Enclosure 12).

discovers that the Government may have incurred such liability on account of the activities of the FRA, the Inspectorate is under an obligation to submit a report to the Chancellor.[98] The Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden*) – the oversight body supervising the law enforcement agencies – is under a similar obligation.[99]

124. In the Chancellor of Justice Instructions Ordinance, the Government has instructed the Chancellor to examine reports from the Commission on Security and Integrity Protection and determine if the State may have incurred liability for damages. If so, the Chancellor must give the concerned individuals an opportunity to submit claims for damages.[100] The Government has not, however, given the Chancellor any instructions as to how to deal with equivalent reports from the Inspectorate.

125. Crucially, providing an individual with an opportunity to submit a claim for damages would inevitably involve advising them of the unlawful conduct, which is tantamount to notification and thus presumably precluded by secrecy. Awarding compensation without informing the individual about the grounds for doing so is also problematic, particularly for want of a legal basis for such a procedure. Consequently, the lack of instructions from the Government on how the Chancellor shall deal with reports from the Inspectorate further seriously undermines the adequacy of the Chancellor's remedial function.

126. The Government has not presented any evidence to demonstrate the effectiveness of the Chancellor as a remedy in this context. The Chancellor can not, therefore, be deemed an effective remedy in the present Case.

(vii) Action for damages, including compensation for violations of the Convention is not an effective remedy

127. Moreover, the prospects of success in bringing an action for damages against the Government are, in practice, highly confined. It is virtually impossible for the individual to discharge its burden of proof in a civil suit against the Government in absence of any

[98] Section 15 of the Foreign Intelligence Inspectorate Instructions Ordinance (*Förordning med instruktion för Statens inspektion för försvarsunderrättelseverksamheten;* 2009:969) (Enclosure 15).

[99] Section 20 of the Commission on Security and Integrity Protection Instructions Ordinance (*Förordning med instruktion för Säkerhets- och integritetsskyddsnämnden*; 2007:1141) (Enclosure 16).

[100] Section 11 of the Chancellor of Justice Instructions Ordinance (*Förordning med instruktion för Justitiekanslern;* 1975:1345) (Enclosure 17).

notification or other effective form of access to documents relating to the contested surveillance.[101] The Government has failed to provide any examples or convincing evidence to demonstrate the effectiveness of this remedy.

(viii) The Parliamentary Ombudsmen is not an effective remedy

128. The Chamber correctly noted that there is also a possibility of addressing an individual complaint to the Ombudsmen. Like the Chancellor, the Ombudsmen is authorised to initiate criminal or disciplinary proceedings against public officials for actions taken in the course of their duties. As with the Chancellor, the Ombudsmen may not issue legally-binding decisions. By contrast to the Chancellor, however, the Ombudsmen is not authorised to grant compensation.

129. The remedial function of the Ombudsmen is negligible at best. It cannot issue legally-binding decisions or grant compensation or award any other form of redress, and that investigations by the Ombudsmen into the activities of the FRA is, as pointed out under section 2.4.8 above, highly unlikely. The Government has not shown any concrete examples or convincing evidence to the contrary. This general remedy must thus be deemed to be of no practical relevance to the present Case.

(ix) A data subject request to the FRA is not an effective remedy

130. Upon request, the FRA is required to inform an individual whether personal data concerning him or her has been processed. This obligation does not apply if the information is covered by secrecy. A decision by the FRA not to disclose any information can be appealed to the Administrative Court in Stockholm.[102]

131. The Administrative Court might, however, not be able to gain access to the necessary classified documents in order to carry out such a review. If documents contain information subject to defence secrecy or secrecy for the protection of international

[101] *Cf. Roman* Zakharov, cited above, § 296.

[102] See in further detail Chamber Judgment, §§ 47–49.

relations, the Administrative Court will only be able to access the documents if the FRA permits it[103] or if the Government so decides.[104]

132. As the Chamber correctly assumed, strict secrecy would not only preclude information on the processing of personal data from being given to requesting individuals,[105] the Administrative Court would also be unable to review the secrecy assessment of the FRA. Consequently, the Applicant agrees with the Chamber's finding that this remedy cannot be deemed to have any practical importance.[106] In any case, it is not available to legal persons, such as the Applicant.

(x) Neither the FRA's procedure to correct, block or destroy personal data nor a complaint to the Data Protection Authority are effective remedies

133. Following a request from an individual who has had personal data registered, the FRA shall promptly correct, block, or destroy personal data that has not been lawfully processed. Under certain circumstances, the FRA must also notify any third party who has received the data.[107] As the Chamber found, this procedure is dependent on the individual's knowledge that personal data has been registered and the nature of that data. Due to secrecy, this remedy must be considered ineffective in practice.[108]

134. An individual may lodge a complaint to the Data Protection Authority. However, the Data Protection Authority cannot by itself order the erasure of unlawfully processed data, but must apply for such a measure to the Administrative Court.[109] By its own admission, the Administrative Court has never received such an application.[110] As pointed out above, the Administrative Court does not have full access to classified documents. The Government has failed to provide any example or convincing evidence to shed light on the

[103] Section 20 of the Administrative Court Procedure Act (*Förvaltningsprocesslagen*; 1971:291) (Enclosure 18); and Chapter 38, section 8 of the Swedish Code of Judicial Procedure (*Rättegångsbalken*; 1942:740) (Enclosure 19).

[104] Chapter 10, section 6 The Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslag*; 2009:400) (Enclosure 20).

[105] Chamber Judgment, § 175

[106] Chamber Judgment, § 175.

[107] Chapter 2, section 4 of the FRA Personal Data Processing Act (Enclosure 8).

[108] Chamber Judgment, § 175.

[109] Chapter 5, section 4 of the FRA Personal Data Processing Act (Enclosure 8).

[110] Email from the Administrative Court dated on 24 April 2019 (Enclosure 21).

effectiveness of this remedy. In keeping with the Court's finding in *Segerstedt-Wiberg* on this remedy, it too must be deemed ineffective.[111]

(xi) Reporting a matter for prosecution is not an effective remedy

135. Finally, the Government has suggested that an individual can report a matter for prosecution. Again, secrecy stifles efficacy. Without knowledge of wrongdoing, the individual has nothing concrete to report to the prosecutor.[112] In addition, prosecution of public officials only afford individual with limited redress in response to them being subjected to unlawful surveillance.

(xii) Existing remedies are ineffective both individually and collectively

136. In conclusion, the effectiveness of the limited, and in many case general, remedies pointed to by the Government is undermined by the fact that individuals will never know whether they have been subject to unlawful surveillance measures. None of the remedies referred to by the Government can be used by an individual to obtain an effective examination of whether they have been subjected to unlawful surveillance and, if so, be granted appropriate redress. The Government has, therefore, not meet its burden of proof.

137. As has been noted by the Court in previous cases on the review afforded by the Chancellor and the Ombudsmen, their "main weakness […] is that, apart from their competence to institute criminal proceedings and disciplinary proceedings, they lack the power to render a legally binding decision. In addition, they exercise general supervision and do not have specific responsibility for inquiries into secret surveillance."[113]

138. The existing remedial bodies are only capable of taking measures to stop or remedy any detected breaches of law and to bring those responsible to liability to a very limited extent. Their respective shortcomings do not cancel each other out, but are cumulative. The sum of several ineffective remedies in this particular context does not, the Applicant submits, equal an effective remedy. Thus, existing remedies are ineffective both individually and collectively.[114]

---

[111] *Cf. Segerstedt-Wiberg and Others*, cited above, § 120.

[112] *Cf. Roman Zakharov*, cited above, §§ 297–298.

[113] *Segerstedt-Wiberg and Others*, cited above, § 118; and *Leander*, cited above, § 82.

[114] See, *e.g.*, Partially Dissenting Opinion of Judges Pettiti and Russo in *Leander*, cited above, p. 32.

(xiii) Therefore, the Government has eschewed an important safeguard against the improper use of its signals intelligence regime

139. Correspondingly, by failing to incorporate effective remedies in its signals intelligence regime, the Government has eschewed an important – if not the most important – safeguard against the improper use of signals intelligence powers.

140. In the Applicant's submission, the lack of an effective notification system and adequate *ex post factum* remedies would in itself constitute a breach of the Convention regardless of the surveillance regime under review.

141. In the context of untargeted bulk interception, remedial deficiencies are particularly concerning since prior review is inevitably carried out at a more abstract level than when there are predefined targets. Accordingly, greater emphasis must be placed on the subsequent review and remedies. A bulk interception regime that fails to incorporate effective remedial mechanisms cannot under any circumstances, the Applicant therefore submits, be considered compatible with the Convention.

142. In case the Court, nevertheless, were to find the Swedish system compatible with Article 8 in its overall assessment of the regime, the Applicant submits that the ancillary but autonomous character of Article 13 of the Convention demands a separate examination of the Applicant's complaints relating to the lack of effective remedies.

2.4.10 The Swedish signals intelligence regime does not satisfy the applicable Convention standards and breaches Article 8 of the Convention

143. In conclusion, the Swedish system lacks several of the minimum safeguards necessary to pass muster under Article 8:

a) there is no clear indication in law of the circumstances in which a warrant must be cancelled, and specifically, no obligation;
b) the scope of the prior judicial review is insufficient; there is no requirement of reasonable suspicion, the materiality threshold is insufficient and there is no possibility for the authorising body to assess the necessity of intended subsequent use of collected data;
c) the supervisory bodies largely lack the necessary power to render legally binding decisions; and

d) there are no effective remedies for individuals who suspect that their communications have been unlawfully intercepted.

144. For the these reasons, the Court is respectfully asked to find that the Swedish signals intelligence regime violates the Applicant's rights under Article 8 of the Convention.

C. Merits: Conditions for communicating data to other parties

1 Introduction

145. In the proceedings before the Chamber, the Applicant submitted that the conditions for communicating intercepted data to other parties affords a wide discretion to the FRA. This, the Applicant submitted, was specifically the case in relation to the communication of data to foreign governments and international organisations.[115]

146. Question 3 of the Court's Questions states:

> "In that connection, to what extent and in what manner is the legal regime applicable in Sweden to communicating intercepted data to other parties capable of interfering with the rights of concrete individuals or organisations under Article 8 § 1 of the Convention? Insofar as it is capable of doing so, is that regime in accordance with the law and necessary within the meaning of Article 8 § 2? To what extent do the standards developed in the Court's case-law on secret measures of surveillance — and, in particular, the interception of communications – apply to this regime?"

2 The existence of an interference

147. As concluded above (see section B.1) the mere existence of the Swedish signals intelligence regime amounts to an interference with the Applicant's rights under Article 8 of the Convention. For the same reasons, so does the legal regime governing the communication of data to foreign governments and international organisations.

3 The justification of the interference

3.1 The applicable test

148. In its review of the British intelligence sharing regime in *Big Brother Watch*, the Court found that Contracting States may not enjoy an unfettered discretion to *request* interception of communications or the conveyance of intercepted communications from non-Contracting States. If that were the case, Contracting States could circumvent their obligations under domestic law or under the Convention.[116]

---

[115] See *inter alia* Chamber Judgment, § 148.

[116] *Big Brother Watch and Others*, cited above, § 424.

149. The Applicant submits that the same holds true, *mutatis mutandis*, when Contracting States *communicate* intercepted data to foreign governments or international organisations. Contracting States can, for instance, outsource processing, storage and analysis of data that would be impermissible under domestic law to a foreign government not bound by similar legal constraints or outsource use that would be impermissible under the Convention to a non-Contracting State.

150. Interpreting the Convention so as to allow Contracting States to avoid responsibility by outsourcing rights-violating conduct would be incompatible with the underlying principles of the Convention.[117] It logically follows from these principles that acts, such as the communication of data, which facilitates treatment contrary to the Convention by another state is directly prohibited by the Convention. The prohibition on transfers of individuals to a state where they may face risk of treatment contrary to the Convention – normally contrary to Article 2 or 3 – is a forthright example of this.[118]

151. Thus, the minimum safeguards that the Applicant submits must apply when communication data to foreign governments and international organisations: (1) accessible legal provisions governing the communication of data to foreign governments or organisations; (2) sufficiently clear conditions on when data may be communicated set out in statute law, including an obligation for the government to take reasonable steps to ensure that the receiving party protects the data with similar safeguards as those applicable to the government; and (3) sufficient supervisory and remedial mechanisms capable of keeping the interference to what is necessary in a democratic society.

3.2 Application of the applicable standards to the present Case

3.2.1 Accessibility

152. The Applicant does not dispute that all legal provisions relating to communication of data have been officially published and are accessible to the public.

[117] See *inter alia Airey v. Ireland*, 9 October 1979, § 24, Series A no. 32 (effectiveness) and *Kjeldsen, Busk Madsen and Pedersen v. Denmark*, 7 December 1976, § 53, Series A no. 23 (general spirit).

[118] See *inter alia Soering v. the United Kingdom*, 7 July 1989, Series A no. 16; and *Saadi v. Italy* [GC], no. 37201/06, ECHR 2008.

3.2.2 Conditions for communicating data

153. The Applicant submits that the discretion granted to the FRA is not sufficiently circumscribed in order to prevent the Government from circumventing domestic law or its obligations under the Convention. Whereas national interests are taken into account, the legislation does not indicate that possible harm to the individual concerned must be considered. Furthermore, as pointed out by the Chamber, the legislation only in very broad terms mentions that 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.[119]

154. The only concrete limits on the FRA's intelligence sharing arrangements are contained in an internal policy document. This document stipulates, *inter alia*, that international cooperation may not be used to circumvent domestic law and policy; that foreign partners may not have direct access to the FRA's databases; and that data shall be communicated only if the recipient agrees to respect Swedish legislation.[120] These guidelines can, however, easily be changed and no oversight body is vested with powers and competence to exercise control over whether these conditions are met and take measures to stop or remedy detected breaches and bring those responsible to liability.

155. In conclusion, the Swedish legislation does not set out the conditions for communicating data in such a way as to minimise the risk of abuse and circumvention of domestic law and the Convention.

3.2.3 Supervision and remedies

156. While the Chamber found that the "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", it considered that "on the whole, the supervisory elements of the system sufficiently counterbalanced the regulatory shortcomings".[121] The Applicant submits that the supervision and the available remedies are ineffective and not in any way capable of

[119] Chamber Judgment, § 150.

[120] FRA, *Övergripande riktlinjer för samverkan med utländs samarbetspartner inom försvarsunderrättelse- och utvecklingsverksamheten,* Bilaga till beslut 10, 120:3011/15:1 (Enclosure 22).

[121] Chamber Judgment, § 150.

counterbalancing the wide discretion of the FRA. The Government has not provided any evidence to the contrary.

157. The Data Protection Authority has never reviewed the FRA's communication of data to foreign governments and international organisations.[122] Furthermore, the Inspectorate, although it shall be kept informed of the FRA's intelligence sharing arrangements[123], cannot carry out any effective review because of the wide discretion afforded to the FRA. Indeed, as the Venice Commission has held "[w]here a power is framed in broad terms in a statute, and oversight is limited to checking if an agency remains within its statutory mandate, then the oversight is of limited use.[124]

158. Moreover, no other remedies are available in relation to communication of data to foreign governments or international organisations than the remedies described in section 2.4.9 above. Accordingly, there are no effective remedies.

159. Lastly, the Applicant would like to refer the Court to a 2016 report by the United Nations Human Rights Committee (the "**Committee**").[125] In the report, the Committee expresses concerns about the limited degree of transparency with regard to the scope of the FRA's surveillance powers and as for the safeguards on their application.

160. The Committee raised specific concerns with regards to the lack of sufficient safeguards against arbitrary interference with the right to privacy in relation to the sharing of raw data with other intelligence agencies. The Committee recommended Sweden to ensure that its intelligence sharing regime is in full conformity with its obligations under the International Covenant on Civil and Political Rights, to ensure that effective and independent oversight mechanisms over intelligence sharing are put in place and that affected persons have proper access to effective remedies in case of abuse.[126] The Government has not acted upon the recommendations by the Committee.

---

[122] See email from the Data Protection Authority dated on 26 April 2019 (Enclosure 23).

[123] Section 6 of the Foreign Intelligence Ordinance (*förordning om försvarsunderrättelseverksamhet; 2000:131*) (Enclosure 24).

[124] Venice Commission Report 2015, para. 93 (Enclosure 1).

[125] UN Human Rights Committee, *Concluding observations on the seventh periodic report of Sweden,* 28 April 2016, CCPR/C/SWE/CO/7 (Enclosure 25).

[126] UN Human Rights Committee, *Concluding observations on the seventh periodic report of Sweden,* 28 April 2016, CCPR/C/SWE/CO/7, para. 37 (Enclosure 25).

161. In conclusion, the Applicant submits that neither the supervision nor the remedies are effective. Consequently, they are incapable of ensuring that the interference caused by the FRA's communication of data to foreign governments and international organisations is kept to what is necessary in a democratic society.

3.2.4 Conclusion

162. For the aforementioned reasons, the Court is respectfully asked to find that the Swedish regime governing communication of data to foreign governments and international organisations gives rise to a violation of Article 8 § 1 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

D. Admissibility

163. The Applicant also complains that Sweden's signals intelligence regime violates its right to an effective remedy under Article 13 of the Convention.

164. Article 13 is engaged if the Applicant's grievances are deemed arguable under the Convention.[127] In the Applicant's submission, it is sufficient that it is possible that the Applicant's communications have been intercepted under the applicable legal regime in order for the Applicant to have an "arguable claim". A stricter requirement in the context of signals intelligence would risk reducing Article 13 to a nullity.[128]

E. Merits

165. In this specific context, Article 13 requires the State to provide a remedy that is "as effective as can be, having regard to the restricted scope for recourse inherent in any system of secret surveillance".[129]

166. A comparison with the IPT in the United Kingdom illustrates that the Swedish remedies are not as effective as can be in this context. In contrast to the individual remedies available in Sweden, the IPT can examine individual complaints from any person who

[127] See *inter alia Boyle and Rice v. the United Kingdom,* 27 April 1988, §§ 52 and 55, Series A no. 131.

[128] *Cf. Klass and Others,* cited above, § 35.

[129] See *inter alia Klass and Others*, cited above, § 69; *Leander*, cited above, § 78; *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 99; and *mutatis mutandis*, *Chahal*, cited above, § 150.

suspect that their communications have been intercepted and "quash any interception order, require destruction of intercept material and order compensation to be paid".[130]

167. For these reasons, the Court is respectfully asked to find a violation of the Applicant's rights under Article 13, separate from Article 8, unless the Court finds a violation of Article 8 at least partly because of a lack of effective remedies.

CONCLUSION

168. For the reasons set out above, the Court is respectfully invited to find that the Government has violated the Applicant's rights under Article 8 § 1 and, depending on the Court's assessment of Article 8, under Article 13.

FREDRIK BERGMAN
Counsel for the Applicant
Head, Centrum för rättvisa

ANGELA EVANS
Counsel for the Applicant

ALEXANDER OTTOSSON
Counsel for the Applicant

EMILIA PALM
Advisor to the Applicant

[130] See *Kennedy*, cited above, §§ 167 and 196; see also *Big Brother Watch and Others*, cited above, §§ 379, 381 and 383.

List of Enclosures

No	Description
1	Venice Commission Report 2015: CDL-AD(2015)011-e, *Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session* [Venice, 20–21 March 2015]
2	European Union Agency for Fundamental Rights, 2017, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: Field perspectives and legal update*
3	Judgment of 21 December 2016, Joined Cases *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, ECLI:EU:C2016:970
4	Advocate General Henrik Saugmandsgaard Øe's Opinion of 19 July 2016, Joined Cases *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, ECLI:EU:C:2016:572
5	Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, CETS No.108
6	Comments by the Foreign Intelligence Inspectorate on legislative proposal Ds 2018:35, 15 November 2018
7	Signals Intelligence Act (*lagen om signalspaning i försvarsunderrättelseverksamhet;* 2008:717)
8	FRA Personal Data Processing Act (*lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*; 2007:259)
9	Report of the Data Protection Authority, 24 October 2016, *Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*
10	Report of the Data Protection Authority, 6 December 2010, *Datainspektionens redovisning av regeringsuppdraget,* Fö 2009/355/SUND
11	Excerpt from prop. 2008/09:201, *Förstärkt integritetsskydd vid signalspaning*, p. 114
12	Letter from the Chancellor of Justice dated on 8 April 2019
13	Email from the Parliamentary Ombudsmen dated on 5 April 2019
14	Ordinance concerning the administration of claims for damages against the Government *(förordningen om handläggning av skadeståndsanspråk mot staten*; 1995:1301)
15	Foreign Intelligence Inspectorate Instructions Ordinance (*förordning med instruktion för Statens inspektion för försvarsunderrättelseverksamheten;* 2009:969)
16	Commission on Security and Integrity Protection Instructions Ordinance (*förordning med instruktion för Säkerhets- och integritetsskyddsnämnden*; 2007:1141)
17	Chancellor of Justice Instructions Ordinance (*förordning med instruktion för Justitiekanslern;* 1975:1345)
18	Administrative Court Procedure Act (*förvaltningsprocesslagen;* 1971:291)
19	Excerpt from Swedish Code of Judicial Procedure (*rättegångsbalk;* 1942:740), Chapter 38
20	Excerpt from the Public Access to Information and Secrecy Act (*offentlighets- och sekretesslag*; 2009:400), Chapter 10
21	Email from the Administrative Court dated on 24 April 2019
22	FRA, *Övergripande riktlinjer för samverkan med utländska samarbetspartner inom försvarsunderrättelse- och utvecklingsverksamheten*, Bilaga till beslut 10, 120:3011/15:1
23	Email from the Data Protection Authority dated on 26 April 2019
24	Foreign Intelligence Ordinance (*förordning om försvarsunderrättelseverksamhet;* 2000:131)
25	UN Human Rights Committee, *Concluding observations on the seventh periodic report of Sweden*, 28 April 2016, CCPR/C/SWE/CO/7