CENTRUM FÖR RÄTTVISA

Stockholm, 19 September 2018

IN THE EUROPEAN COURT OF HUMAN RIGHTS

Application no. 35252/08

CENTRUM FÖR RÄTTVISA

("Applicant")

v.

SWEDEN

("Government")

REQUEST FOR REFERRAL TO THE GRAND CHAMBER ON BEHALF OF THE APPLICANT

I. INTRODUCTION AND SUMMARY

1. The Applicant respectfully requests the Panel of the Grand Chamber of the European Court of Human Rights (the "Panel") to refer the case of *Centrum för rättvisa v. Sweden* (application no. 35252/08) (the "Case") to the Grand Chamber of the European Court of Human Rights (the "Grand Chamber"), in accordance with Article 43 of the European Convention on Human Rights (the "Convention").

2. The Case is about what minimum safeguards should govern the use of the bulk interception of electronic signals for national security purposes. Member States of the Council of Europe ("Member States") face serious threats from terrorism, criminal activity, and hostile actors. Interception activities form part of how Member States counter these threats. Without proper safeguards, however, the use of bulk interception risks intruding upon the very basic fundamental rights and freedoms of the societies that such surveillance seeks to protect.

3. The right to privacy is arguably the defining human rights challenge of the digital age. Article 8 of the Convention requires clear and robust safeguards to be laid down by the Grand Chamber that keep apace with the rapid advancements in surveillance technology and use, and that make clear whether and how bulk interception activities can be safeguarded against intentional or inadvertent abuse.

4. *Centrum för rättvisa v. Sweden* (no. 35252/08, 19 June 2018) and *Big Brother Watch and Others v. the United Kingdom* (nos. 58170/13, 62322/14, 24960/15, 13 September 2018) are the first

cases in which the European Court of Human Rights (the "Court") have examined the use of bulk interception regimes used exclusively within the field of national security. The rulings in these cases, the Applicant respectfully submits, require further judicial examination by the Grand Chamber in order to clarify and re-examine the safeguards that apply to such interception regimes.

5. The Applicant submits that this Case involves several serious questions "affecting the interpretation or application of the Convention or the Protocols thereto, or a serious issue of general importance" within the meaning of Article 43(2) of the Convention, and therefore submits that the Panel must, with regard to its obligation under this provision, refer the Case to the Grand Chamber. Specifically, the Applicant requests that the Grand Chamber take this opportunity to:

(1) Clarify the necessary minimum safeguards under Article 8 of the Convention for a bulk interception regime dealing exclusively with national security, in light of the ambiguity and potential inconsistency between the rulings of the Third and the First Sections of the Court in *Centrum för rättvisa* and *Big Brother Watch* respectively;

(2) Re-examine the Court's exclusion of the "reasonable suspicion" requirement laid out in *Roman Zakharov v. Russia* [GC] (no. 47143/06, 4 December 2015, § 262, ECHR 2015–VIII) from the mandatory minimum safeguards for bulk interception regimes, to ensure the same procedural safeguard is afforded, where possible and appropriate, to bulk interception regimes as in targeted interception activities;

(3) Develop the role of independent judicial oversight in the necessary minimum safeguards; and

(4) Develop the minimum safeguards governing inter-state intelligence sharing.

II. PROCEDURAL BACKGROUND

A. The Applicant

6. The Applicant is a non-profit public interest law firm based in Stockholm, Sweden, that seeks to protect and promote individual rights and freedoms. It represents private individuals in public interest litigation proceedings, runs educational outreach programs, and participates in the public debate on civil liberties.

B. National proceedings

7. The Applicant did not initiate prior national proceedings. The Court held in *Centrum för rättvisa* that the Applicant was not required to bring any domestic proceedings under Article 35 of the Convention in light of the absence of any effective domestic remedy (*Centrum för rättvisa,* cited above, § 84).

C. Chamber proceedings

8. On 14 July 2008, the Applicant lodged its application to the Court in accordance with Article 13 of the Convention. It submitted that:

(1) Swedish state practice and legislation concerning signals intelligence had violated and continued to violate its right to

respect for private life and correspondence under Article 8 of the Convention; and

(2) that Sweden was in violation of Article 13 of the Convention, given its failure to afford the Applicant an effective remedy.

9. On 19 June 2018, the Third Section of the Court, sitting as a Chamber, delivered its judgment. It held that the Swedish system of bulk interception revealed no significant shortcomings in its structure and operation that amounted to a violation of Article 8 of the Convention. At the same time, however, the Court stressed that the relevant Swedish law and practice gave "some cause for concern with respect to the possible abuse of the rights of individuals", and that there was "scope for improvement" – notably the regulation of the communication of personal data to other states and international organisations and to the practice of not giving public reasons following a review of individual complaints (*Centrum för rättvisa*, cited above, §§ 150, 173 and 177).

III. REASONS FOR REFERRING THE CASE TO THE GRAND CHAMBER

A. Introduction

10. Article 43(2) of the Convention states that the Panel shall refer a case to the Grand Chamber for judgment if it "raises a serious question affecting the interpretation or application of the Convention or the Protocols thereto, or a serious issue of general importance". The Applicant submits that this cases raises such questions. This is set out in the following sections.

11. Specifically, the Grand Chamber is invited to:

(1) Clarify the necessary minimum safeguards for a bulk interception regime dealing exclusively with national security;

(2) Re-examine the Court's exclusion of the reasonable suspicion requirement from the minimum safeguards for bulk interception;

(3) Develop the role of independent judicial oversight as part of the minimum safeguards that apply to bulk interception regimes; and

(4) Develop the minimum safeguards governing inter-state intelligence sharing.

B. The Grand Chamber is invited to clarify the necessary minimum safeguards for a bulk interception regime dealing exclusively with national security

12. The Applicant invites the Grand Chamber to clarify the minimum safeguards under Article 8 of the Convention applicable to bulk interception regimes used for national security purposes, in light of the ambiguities in the Court's adaptations of safeguard requirements from other types of interception activities, namely the use of targeted secret surveillance in criminal investigations.

13. The Court has recognised the need to afford states a margin of appreciation in the design of their interception regimes in order to protect national security. The use of bulk interception may fall within this margin (*see Centrum för rättvisa*, cited above, § 112, and *Big Brother Watch*, cited above, § 314, *cf. Weber and Saravia* (dec.), no. 54934/00, 29 June 2006 and *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008).

14. Nevertheless, the Court must be satisfied that domestic law ensures that interception regimes are only used when "necessary in a democratic society". To that end, the domestic law must provide for adequate and effective safeguards and guarantees against abuse (*Zakharov,* cited above, § 236).

15. The Court's jurisprudence, however, is not clear as to what constitutes adequate and effective safeguards in relation to the present kind of bulk interception regimes dealing exclusively with national security.

16. In the context of interception activities forming part of a criminal investigation, the Court has developed the following six minimum safeguards:

(i) a description of the nature of offences which may give rise to an interception order;

(ii) a definition of the categories of people liable to have their communications intercepted;

(iii) a limit on the duration of the measures;

(iv) the procedure to be followed for examining, using and storing the data obtained;

(v) the precautions to be taken when communicating the data to other parties; and

(vi) the circumstances in which recordings may or must be erased or destroyed (*Weber and Saravia*, cited above, § 95, with further references).

17. In 2015, the Grand Chamber in *Zakharov* affirmed that these requirements also apply in cases where the interception activities were carried out for national security purposes (*Zakharov*, cited above, §§ 231 and 232). The Grand Chamber also specified that national laws regulating interception of communications had to have regard to the applicable authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms, and the remedies provided for by national law (*ibid.*, § 238).

18. Since *Zakharov*, *Centrum för rättvisa* is the first case where the question of minimum safeguards was explored within the context of a *bulk* interception regime dealing exclusively with national security. The Court held that the minimum safeguards in *Zakharov* had to be "adapted" (*Centrum för rättvisa*, cited above, § 114), and accordingly presented a reformulation of the safeguards (*ibid.,* §§ 122, 130 and 146).

19. Based on the adapted, and arguably less strict, standards the Court permitted the interception of communications for the purposes of developing the National Defence Radio Establishment's (Sw. *Försvarets radioanstalt*) ("FRA") own signals intelligence technology (*ibid.*, § 122); the Court accepted that the circumstances in which interception must be discontinued are not clearly defined (*ibid*., § 130); and the Court allowed for automated haystacks of "unprocessed information" (*ibid*., § 146). Under the original *Weber* requirements, this would most likely not have been permissible.

20. Crucially, the Court downplayed the importance of requiring that the conditions for communicating the intercepted data to other

parties must be clearly set out, did not attach any practical importance to the requirement for subsequent notification, and did not mention the requirement laid out in *Zakharov* to have "reasonable suspicion" of an individual being associated with a criminal or other act prior to engaging in interception activities (*ibid*., §§ 150 and 175).

21. Just a few months later, in *Big Brother Watch*, the Court formulated the minimum safeguards from *Zakharov* differently, and without reference to the judgment in *Centrum för rättvisa*. Regrettably, these two judgments, therefore, do not lay down a clear and consistent interpretation of how Member States must uphold their obligations under Article 8 of the Convention when conducting bulk interception activities.

22. If bulk interception activities are to be considered as capable of being compatible with Article 8 of the Convention, there must be clearly articulated safeguards. It is the Applicant's submission that this warrants careful judicial examination and clarification from the Grand Chamber. Indeed, in the partly concurring, partly dissenting separate opinion in *Big Brother Watch*, Judge Koskelo joined by Judge Turković, also suggests that the Court's existing case law on this matter is insufficient, and warrants clarification by the Grand Chamber. Specifically, Judge Koskelo states:

> It is obvious that such an activity – an untargeted surveillance of external communications with a view to discovering and exploring a wide range of threats – by its very nature takes on a potentially vast scope, and involves enormous risks of abuse. The safeguards against those risks, and the standards which under the Convention should apply in this regard, therefore raise questions of the highest importance. I am not convinced, in the

> light of present-day circumstances, that reliance on the Court's existing case-law provides an adequate approach to the kind of surveillance regimes like the one we are dealing with here. A more thorough reconsideration would be called for. I acknowledge that this would be a task for the Court's Grand Chamber. (*Big Brother Watch*, cited above, partly concurring, partly dissenting separate opinion of Judge Koskelo, joined by Judge Turković, § 3).

23. Therefore, the Applicant submits that the Case must be referred to the Grand Chamber in order to provide vital clarification on the safeguards applicable to bulk interception activities. The Applicant also, in particular, wishes to request the Grand Chamber's re-examination of the exclusion or underdevelopment of certain safeguards, as set out in the following sections.

C. The Grand Chamber is invited to re-examine the Court's exclusion of the reasonable suspicion requirement from the minimum safeguards for bulk interception

24. The Applicant specifically requests the Grand Chamber to reconsider the omission of a "reasonable suspicion" requirement, where possible and appropriate, within the context of a bulk interception regime.

25. As recently as 2015, the Grand Chamber held in *Zakharov*, that governments may only intercept communications where the body authorizing the surveillance has confirmed that there is a "reasonable suspicion" of wrongdoing on the part of the persons concerned (*Zakharov*, cited above, §§ 260, 262 and 263, *see also*

Szabó and Vissy v. Hungary, nos. 11327/14, 11613/14, § 71, 12 January 2016).[1]

26. In *Centrum för rättvisa*, however, the Court, without justification, appears to have implicitly excluded the reasonable suspicion requirement from the prior authorisation measures set out in *Zakharov* altogether. This represents either a deliberate departure from the Grand Chamber's established jurisprudence in *Zakharov*, or an unreasoned distinction made between cases of targeted and bulk interception.

27. In *Big Brother Watch*, the Court dispensed with the requirements in *Zakharov* (i) to require reasonable suspicion against a targeted individual; and (ii) to ensure that individuals having been personally targeted were issued with subsequent notification. The Court stated that "bulk interception is by definition untargeted and to require 'reasonable suspicion' would render the operation of such a scheme impossible". Similarly, it reasoned that "the requirement of 'subsequent notification' assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime". (*Big Brother Watch*, cited above, §§ 316 and 317).

28. Respectfully, this reasoning fails to consider that individuals may nevertheless be indirectly targeted or be implicated in bulk interception activities through the use of personalised search terms. The possibility of using personalised search terms is expressly

[1] The Court further notes that interceptions may be ordered not only in respect of a suspect or an accused, but also in respect of a person who may have information about an offence or may have other information relevant to the criminal case (*Zakharov,* cited above, § 245).

provided for in Section 3 of the Swedish Signals Intelligence Act (Sw. *Lag om signalspaning i försvarsunderrättelseverksamhet*), which states that search terms directly relating to a specific natural persons may be used if it is of exceptional importance for the intelligence activities (*Centrum för rättvisa*, cited above, § 3).

29. Although the Swedish legislation lacks a reasonable suspicion requirement in order to use personalised search terms in this context, it includes a subsequent notification requirement. Section 11a of the Swedish Signals Intelligence Act requires the FRA, after a surveillance mission is concluded, to notify individuals if search terms have been used that directly related to them (*ibid*., § 44).

30. This calls into question the veracity of the Court's assertion in *Big Brother Watch* that reasonable suspicion and subsequent notification are requirements that are *per se* incompatible with a bulk interception regime (*Big Brother Watch*, cited above, § 317). It also gives cause for concern as to why the reasonable suspicion requirement did not form an explicit part of the Court's judgment in *Centrum för rättvisa.*

31. The Applicant submits that the minimum safeguards governing bulk interception should contain a requirement of reasonable suspicion, at least in situations where personalised search terms or other such indicators are used in order to single out or target specific individuals as part of a broader bulk interception activity. The use of search terms directly relating to a specific individual has serious privacy implications. 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.

32. In sum, current jurisprudence either categorically refutes the applicability of the reasonable suspicion test to bulk interception regimes (*Big Brother Watch*), or fails to address the issue directly (*Centrum för rättvisa*). Both approaches risk diluting the robust protections afforded in *Zakharov*. In light of these significant, and in the Applicant's submission potentially harmful, developments in the Court's case law, the Applicant submits that the Grand Chamber should seize the opportunity to examine the issue within the context of the present Case. Sweden's applicable legal framework is especially pertinent to the issue, given that it specifically anticipates personalisation of search queries within the context of bulk interception.

D. The Grand Chamber is invited to develop the role of independent judicial oversight as part of the minimum safeguards that apply to bulk interception regimes

33. The Court has not yet set a requirement for prior judicial authorisation of interception missions. The Applicant submits that due to present-day realities of far-reaching surveillance techniques and prerogatives, the time has come to do so. It cannot be safely assumed that the executive branch of government will be capable of effectively checking itself in this context.

34. 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 (*see Zakharov*, cited above, § 233, and *Klass and Others v. Germany*, 6 September 1978, Series A no. 28, § 55).

35. In *Centrum för rättvisa*, whilst the Court did not deem prior judicial authorisation an absolute requirement under the Convention, it emphasised its crucial role in safeguarding executive acting against arbitrariness (*Centrum för rättvisa*, cited above, § 133). In *Big Brother Watch*, the Court also held that judicial authorisation is an important safeguard, and perhaps even "best practice" (*Big Brother Watch*, cited above, § 320).

36. The reluctance of the Court in *Centrum för rättvisa* and *Big Brother Watch* to recognise prior judicial authorisation as an essential safeguard is regrettable. As the Venice Commission of the Council of Europe has observed, many states rely primarily on internal controls in the area of strategic surveillance, which is deemed insufficient. According to the Commission, external oversight over signals intelligence need to be considerably strengthened (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], para. 21).[2]

37. Arguably, if authorising surveillance is left to the executive branch there is a great risk of it erring on the side of over-collecting

[2] The report is available online at: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e.

intelligence and discounting individual rights. The executive cannot sufficiently check itself in this context. The Grand Chamber 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.

E. The Grand Chamber is invited to develop the minimum safeguards that govern inter-state intelligence sharing

38. The Grand Chamber is further invited to specify the relevant criteria for assessing whether sufficient safeguards are in place in the context of inter-state intelligence sharing.

39. Previously, the Court has merely stated that the precautions to be taken when communicating data to other states should be set out in statute law (*Weber and Saravia*, cited above, § 95 and *Centrum för rättvisa*, cited above, § 150).

40. In its proceedings before the Court, the Applicant submitted that the conditions for communicating intercepted data to other parties under Swedish legislation left too much discretion to the FRA and that adequate safeguards against abuse were not in place.

41. The Court concurred that the Swedish legislation contained regulatory shortcomings and held that those shortcomings warranted "some cause for concern with respect to the possible abuse of the rights of individuals". However, the Court stated that the supervisory elements of the legislation sufficiently counterbalanced the regulatory shortcomings identified with respect to inter-state transfers (*Centrum för rättvisa*, cited above,

§ 150). Previous case law is silent on the issue of whether such oversight is even capable of counterbalancing wide discretion in the way the Court suggests.

42. In *Big Brother Watch*, the Court found that if Member States were to enjoy unfettered discretion to exchange intercepted communications with other states, they could circumvent their obligations under the Convention (*Big Brother Watch*, cited above, § 424, *cf*. the Venice Commission report, cited above, para. 74).

43. As such, the Court in *Big Brother Watch* held that minimum safeguards relating to the storage, examination, use, onward dissemination, erasure and destruction of data must not only be present at the interception stage, but also when it comes to inter-state sharing of intelligence (*ibid*, cited above, § 423). Judge Koskelo, in her separate opinion, stated:

> It is easy to agree with the principle that any arrangement under which intelligence from intercepted communications is obtained via foreign intelligence services, whether on the basis of requests to carry out such interception or to convey its results, should not be allowed to entail a circumvention of the safeguards which must be in place for any surveillance by domestic authorities. Indeed, any other approach would be implausible. (Judge Koskelo, cited above, § 30).

44. Fundamentally, sharing intelligence should be accompanied by appropriate safeguards against the risks which such data transfers pose for individuals. The Applicant submits that the Court's current case law on inter-state intelligence sharing is not sufficiently developed, and poses a serious question affecting the interpretation of the Convention.

45. The Grand Chamber is, therefore, requested to explicitly develop the relevant criteria for assessing whether appropriate safeguards are in place in terms of sharing and receiving intelligence with and from third parties, including other states.

F. The Panel is requested to take into account that the case raises an issue of general importance

46. Lastly, the Applicant submits that this case raises a serious issue of general importance, namely the inherent difficulty in balancing individuals' reasonable expectations of privacy and national security in the context of mass digital surveillance and intelligence sharing. This in itself warrants consideration of the case by the Grand Chamber.

47. Today, people live major portions of their lives online. We use the internet for everything. Much of this activity is conducted on mobile digital devices, which are seamlessly integrated into our personal and professional lives. These devices have replaced and consolidated our fixed-line telephones, filing cabinets, notebooks, wallets, photo albums, address books and private diaries.

48. At the same time, technological progress has allowed for the development of surveillance methods that enables the government to peer into the most intimate aspects of peoples' private lives. As this Court has held, the technological developments must be accompanied by a simultaneous development of legal safeguards, securing respect for citizens' Convention rights (*Szabó and Vissy*, cited above, § 68).

49. It would, to cite the Court in *Szabó and Vissy*:

> defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives (*Szabó and Vissy*, cited above, § 68).

50. In all probability, mass surveillance, both regulated and unregulated, as well as intelligence cooperation, will only become more common and far-reaching in the future. In fact, the European Agency for Fundamental Rights has recently issued a report that draws this very conclusion (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].

51. It should be recalled that, according to a report by the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly, the documents leaked by Edward Snowden revealed 19 of the 47 Member States to have cooperated with the United States National Security Agency in conducting mass surveillance of European citizens (*see* Doc. 13734 of 18 March 2015, *Report of the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly*, rapporteur: Mr Pieter Omtzigt, para. 42)[4].

52. Apart from *Centrum för rättvisa* and *Big Brother Watch,* this Court's case law has not dealt with the kind of bulk interception

[3] The report is available online at: http://fra.europa.eu/en/publication/2018/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies.

[4] The report is available online at: http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=21583.

and intelligence sharing we see today, but with regimes which, as a matter of either law or fact, have been narrower in scope. In light of current developments, reliance on the line of existing case law is no longer an adequate basis for assessing the standards which under the Convention should govern this particular domain (*see* Judge Koskelo, cited above, § 4).

53. The current Convention standards are in vital need of clarification and development in order to ensure the Convention framework can achieve a proper balance of privacy and national security in the context of mass surveillance and intelligence-sharing in the digital age. Without robust safeguards, such interception activities pose a threat towards innocent, law-abiding citizens, generating public distrust in government at a time when it is arguably needed more than ever. A thorough reconsideration of the Court's approach by the Grand Chamber is, therefore, warranted also on this ground.

IV. CONCLUSION

54. For the reasons set forth above, the Applicant requests that the case be referred to the Court's Grand Chamber pursuant to Article 43 of the Convention.

55. Should the request be granted, the Applicant would respectfully request that it be afforded the opportunity to make further submissions as to the merits of the Case.

Fredrik Bergman
Head, *Centrum för rättvisa* (Centre for Justice)