European Court of Human Rights
Council of Europe
67075 Strasbourg-Cedex
France

***

# THIRD PARTY INTERVENTION

**in the case**

***Centrum för rättvisa v. the Kingdom of Sweden***
(Application No 35252/08)

**from**

**International Commission of Jurists, Norwegian section**

***

**Intervening party** : International Commission of Jurists, Norwegian section

Representative : [redacted]

Address : c/o Advokatfirmaet Stabell
Rosenkrantzgate 7
0159 Oslo
Norway

**Agent** : [redacted]

Address : Bjørnstjerne Bjørnsons plass 1
0340 Oslo
Norway

Telephone : (+47) 97 06 21 20

Telefax : (+47) 23 04 85 50

E-mail : [redacted]

***

**Contents**

## I INTRODUCTION – REQUEST FOR INVITATION TO SUBMIT WRITTEN COMMENTS THROUGH THIRD PARTY INTERVENTION

1. International Commission of Jurists, Norwegian section (hereinafter referred to as "ICJ-Norway"), wishes to intervene in support of the applicant, Centrum för Rättvisa (hereinafter referred to as "CfR), in the complaint made against The Kingdom of Sweden (hereinafter referred to as "Sweden"), dated 14.07.08, regarding Swedish legislation on general strategic monitoring and potential interception of all electronic communication passing Sweden's borders via air and/or wire.

2. ICJ-Norway, therefore, requests that The President of the Chamber invites ICJ-Norway to submit these written comments in the above-mentioned case, according to the rules on Third Party Intervention as set out in article 36 (2) of the Convention.

3. In addition to declaring general support to CfR's application, ICJ-Norway wishes to supplement the application by highlighting, in particular, the effects of the relevant Swedish legislation on the right of privacy – and freedom of expression – of non-Swedish residents/citizens, living in the territories of other High Contracting Parties, such as Sweden's closest neighbor, Norway.

4. In ICJ-Norway's view, and according to the very nature, as well as the expressed, official objective of the Swedish legislation, its adverse effects are both *de facto* and *de jure* far greater vis-á-vis Norwegian citizens, or, indeed, any non-Swedish citizen, than vis-á-vis Swedish citizens. With reference to further elaboration on these points below, in this introductory context attention is drawn to the fact that the subject of the strategic monitoring and interception is "foreign" communications passing Sweden's borders. Furthermore, to the extent that the Swedish legislation provides any system at all for independent, judicial control with the surveillance authorities, or any legal remedies for persons who are subjected to surveillance under the relevant regime, none of these measures or remedies are available to non-Swedish citizens. Such persons, including Norwegian citizens, would, therefore, seem to be not only typical subjects for the surveillance in question, but also basically "lawless" with regard to any legal protection or remedies by which their basic rights to privacy and freedom of expression can be secured.

5. It would, therefore, seem of high importance that the Court is made aware of the details of such a perspective, as part of the basis for its review of the substance of the application in relation to the relevant articles.

6. The further reasons for this intervention, and in particular the more detailed legal observations made by ICJ-Norway, will be elaborated on in the following. However, we find it in good order to start by giving the Court a brief presentation of ICJ-Norway.

## II PRESENTATION OF ICJ-NORWAY

7. The International Commission of Jurists is a non-governmental organisation working to advance understanding and respect for the Rule of Law as well as the protection of human rights throughout the world. It was set up in 1952 and has its headquarters in Geneva, Switzerland. It is made up of 45 eminent jurists representing different justice

systems throughout the world and has 90 national sections and affiliated organisations. The International Commission of Jurists has consultative status at the United Nations Economic and Social Council, the United Nations Organisation for Education, Science and Culture (UNESCO), *the Council of Europe* and the Organisation of African Unity. The organization also cooperates with various bodies of the Organisation of American States and the Inter-Parliamentary Union.

8. ICJ-Norway is one of the International Commission of Jurists' above-mentioned national sections, founded September 4th 2008 in Oslo, Norway, as a non-profit association under Norwegian jurisdiction, with Norwegian Supreme Court Justice Mr. [redacted] as Chairman of the Board.[1]

## III GENERAL FACTS AND MAIN POINTS ON RELEVANT DOMESTIC LAW

9. With regard to the general facts of the case, including the description of the relevant, domestic Swedish law, reference is made to CfR's application (particularly paragraphs 27-42).

10. However, CfR's complaint in it's own name is, understandably, primarily directed towards the Swedish legislation's effect on the rights of Swedish citizens. ICJ-Norway, therefore, wishes to supplement CfR's application on these points, by drawing the Court's attention to how the legislation in question directly and specifically affects non-Swedish citizens, in this case Norwegian citizens in particular.

11. Such a supplementary perspective will be given in chapter IV below, taking into account the afore-mentioned general reference made in paragraph 9 above.

## IV THE NON-SWEDISH PERSPECTIVE

12. As explained more elaborately in CfR's application, the Swedish legislation in question basically authorizes the Swedish authorities to secretly monitor, intercept, review and store the contents of *all* electronic communication passing Sweden's borders – irrespective of whether the communication crossing the borders is initiated in Sweden, terminated in Sweden or just passing through Sweden in transit.

13. This means that any communication between a Norwegian citizen and someone communicating from within Swedish territory would be subject to such control by Swedish authorities. Even communication between a Norwegian citizen and someone *anywhere* outside Norway, would be subject to such control, as long as the communication passes through Sweden.

14. A special report from the Norwegian Postal and Telecom Agency, dated November 2008, was commissioned by the Norwegian Ministry of Communications to get an overview of how electronic communications in and to and from Norway would be affected by the new, Swedish legislation.[2] As described in this report, most of electronic communication in and out of Norway, is indeed routed through Sweden. Even a substantial portion of domestic Norwegian communication, is partly routed

[1] ICJ-Norway's Articles of Association are *enclosed* (**Attachment 1**)

[2] "Notat om "FRA-loven" og ruting av elektronisk kommunikasjon via Sverige", November 2008 – the report is *enclosed* (**Attachment 2**)

through telecommunication infrastructure in Sweden. This is described in detail in the enclosed report, and is also clearly illustrated graphically in the map inserted in chapter 4.1 in the report. Thus, most international communication to and from Norwegian citizens, as well as parts of domestic Norwegian communication, *is/will be* directly affected by the new, Swedish surveillance system – not only in theory, but also very much in practice.

15. Although such reservations are not immediately apparent from the wording of the Swedish legislation (nor relevant from a Norwegian perspective ), the Swedish government has in various forums stated that domestic communication, purely between persons within Sweden's borders, is not subject to the monitoring in question. The government and its representatives have, rather, in these connections stressed that the monitoring has so-called "foreign" communications as its target.[3] As also stressed by the same officials, one of the main objectives of such gathering of intelligence, is to have a better bargaining hand when exchanging intelligence with other countries' authorities. This was, inter alia, confirmed by Sweden's Foreign Minister, [redacted] in an interview with the Swedish public broadcaster, Sveriges Television (SVT) on September 13th 2008.[4] In this interview, [redacted] expressed himself to the effect that if Sweden wanted to participate in league with the "big players" in the international intelligence trade, it would have to be able to offer the kind of intelligence information that the new legislation allowed for the collection of.

16. In other words, not only is communication to and from Norwegian citizens as described in paragraphs 13 and 14 above, directly subject to control in principle; such communication is by category the *explicit target* for the secret monitoring by Swedish authorities, whose objective in their collecting of information is partly to secretly pass it on to other countries' authorities – for instance Norwegian authorities.

17. CfR has in its application correctly pointed out the clear deficiencies of the Swedish legislation with regard to a number aspects;

    - the very wide definition of the term "external threats", which constitutes the very basis for the strategic monitoring and interception of electronic communication in question and which in itself can hardly be said to represent any real limitation. Quite to the contrary, as exemplified through the statements made by relevant, high-ranking Swedish officials (ref. paragraph 15 above), collection of information as potential "collateral" in bi-lateral exchange of information with other states, is a main motivation. Thus, the official view seems to be that any information which might be of interest to another states' authorities, is "fair game", the logic being that not having such information available, would put Swedish authorities at a disadvantage in the unofficial market for intelligence information and thereby, ultimately, jeopardizing Sweden's security;
    - the non-existent regulation of what type of search terms are to be used by the surveillance authorities, except from the provision stating that search terms

[3] See, for instance, the interview with the General Director of the Swedish Surveillance Authority (Försvarets Radioanstalt), [redacted], published on the web-site of the Swedish newspaper Dagens Nyheter: http://www.dn.se/DNet/jsp/polopoly.jsp?d=1042&a=803137

[4] See the relevant excerpt on SVT's web-tv archive-service: http://svt.se/svt/play/video.jsp?a=1246030

directly linked to a specific individual are only to be used when "necessary" for intelligence purposes;

- the lack of foreseeable and clear regulation of how and whether the content of communication which is intercepted, is actually stored, distributed or destroyed;
- the utter lack of independent, judicial control with the governments' and its surveillance authority's practicing of their wide, discretionary powers to monitor, intercept, store and distribute the contents of private individuals' communication;
- the complete absence of remedies for citizens whose communication has, in fact, been subject to interception. The authorities have no obligation at any stage to inform an individual that his or her communication has been subject to interception. The legislation does not even grant an individual who actively enquires about it, a right to demand an answer.

18. These deficiencies are all the more critical for Norwegian citizens. Not only because, as shown above, their electronic communication, by the legislations' and the Swedish authorities' general definition, is the very target for the surveillance in question, but also because any safeguards which may exist against arbitrariness or, indeed, deliberate misuse of power on part of the Swedish authorities, pertain only to Swedish citizens. Foreigners, including Norwegians, are for all practical purposes *lawless*.

19. This becomes very apparent when one reviews the Swedish government's reaction to the massive public protests against and critique of, inter alia, the deficiencies mentioned above in paragraph 17.

20. The government eventually responded by issuing a press release on September 25th 2008, in which it announced that it would seek to accommodate some of the critical comments, by introducing improvements to the legislation with regard, inter alia, to limiting the discretionary powers on the one hand, and to introducing a more "judicial-like" control with the surveillance activity. One specific point mentioned was introducing a requirement to seek special permission from a "judicial-like" authority, before using search terms directly linked to a specific individual in the monitoring of communication. Some time later, an internal government document (power point-presentation for the Cabinet of Ministers) was leaked to the press, and subsequently published *in extenso* by several media on the web.[5] The internal Cabinet presentation explains and proposes in further detail how the announced improvements in the vaguely worded press release could be transformed into formal legislation.

21. Through reading that document, it is quite obvious that the possible improvements seek only to safeguard the rights of Swedish citizens. For instance, with regard to the above-mentioned special permission as a condition for using search terms directly linked to a specific individual, this is described as applicable only if the individual in question is a Swedish *resident* (re. the Swedish phrase "person med hemvist i Sverige"). Also other possible safeguard amendments mentioned in the document are explicitly limited in scope to safeguarding the personal integrity of Swedish residents.

[5] "Signalspaningslagen – Statsrådsberedningen, Regeringskanseliet", which is *enclosed* (**Attachment 3**)

22. In conclusion, even taking into account that the Swedish Government actually does propose supplementary provisions in line with the announced amendments to the Acts in question, and Parliament subsequently sanctions them, Norwegian citizens – or any other citizens of any High Contracting State outside Sweden – are still left lawless as under the present legislation. They are faced with the constant risk that their private communications which happen to pass Sweden's borders could be subject to interception and subsequently stored, distributed and misused by and at the absolute discretion of the Swedish authorities. Furthermore, as substantiated above, the information could just as likely become an object of trade with other states' authorities, including the authorities of the same citizen's state, in circumvention of any domestic legislation restricting the same authorities from gathering such information through "ordinary" channels.

## V COMMENTS REGARDING APPLICATION OF THE CONVENTION

23. As stated in the introductory comments in chapter I above, ICJ-Norway generally supports CfR's application. ICJ-Norway also fully agrees with CfRs views and arguments with regard to the application of Articles 8 and 13 in the present case, including the references made to the Court's relevant case law. The Court's recent judgment in *Liberty and others v. The United Kingdom* [6] seems particularly relevant in this context.

24. However, ICJ-Norway would suggest that the Court, in reviewing CfR's application, also takes into consideration the wider perspective described in chapter IV above, and the further consequences of doing so with regard to securing an effective enforcement of the basic human rights guaranteed by the Convention to all individuals within the jurisdiction of the Court.

25. ICJ-Norway would like to elaborate on some main points in this respect:

26. Although a High Contracting State, such as Sweden in the present case, according to Article 1 of the Convention, might not have a direct obligation to secure the rights of citizens outside their jurisdiction, this does not mean that the *negative obligations* to abstain from interference with for instance the right to respect for privacy and correspondence are not applicable also with respect to citizens of High Contracting States outside their jurisdiction.

27. The need for such an interpretation of the Convention seems particularly apparent in the present case, where the explicit targets for the interference by definition are citizens of Sweden's neighboring jurisdictions – and where one of the expressly stated objectives is to obtain information which can be traded with for instance the authorities of the same citizen's state.

28. Taking a contrary view would, in principle, allow for all the High Contracting States to enact similar surveillance legislation, providing the rights of their own citizens are respected, and thereby be able to monitor and intercept all other citizens' communication "on behalf of" the respective neighboring states' authorities, by putting the inter-state trading of gathered information in system – effectively

[6] 01.07.08 (Application no. 58243/00)

circumventing not only the individual rights set out in the Convention, but also undermining the whole idea upon which the Convention is based.

29. Such a scenario becomes even more disturbing, when seen in conjunction with other European legislation which is presently being implemented in most of the High Contacting States. The European Union's Directive 2006/24/EC, on "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC", is the obvious reference on this point. Through the implementation of this Directive, all EU and EFTA member states will in principle have access to all information regarding electronic communication between individuals in Europe (Who communicated with who? By what means? At which times? From which geographical position?), apart from the actual contents of the communication.

30. Normally, getting access to the actual contents of such communication requires that the relevant authorities – in practice the police – follow the judicially supervised, and generally strict, procedures set out in the respective jurisdictions' criminal procedure legislation. If, however, the sort of intelligence information that the Swedish legislation allows for the gathering of is readily available through the secret and unofficial channels of international intelligence cooperation, one would be naive in not presuming that such opportunities would be exploited by the relevant authorities.

31. ICJ-Norway is, of course, not calling upon the Court to take a view on other European legislation as such in the present case. ICJ-Norway is merely suggesting that the existence of such legislation is a *fact* which should be taken into consideration in the Court's assessment of the potential impact of the Swedish legislation in question in the present case.

32. Another point which ICJ-Norway would ask the court to bear in mind when reviewing CfR's application, is that the interference with private communication represented in the present case, also has an obvious potential chilling effect on the freedom of expression, as protected by Article 10 of the Convention.

33. Whereas Article 8, in effect, protects freedom of expression within the private sphere, there is a close relationship between this aspect of respect for privacy and correspondence and freedom of expression in relation to public exchange of information and ideas, guaranteed in Article 10. This becomes most apparent when considering the relationship between journalists and their sources, and the journalists' right to protect the identity of those sources.[7]

34. In today's society it is commonplace for journalists to communicate with sources in other jurisdictions, and such transfrontier communication is mostly conducted via various forms of electronic communication media (mobile phone, e-mail etc.). From a Norwegian perspective, it is obvious that Norwegian journalists communicate on a daily basis particularly with sources in Sweden and other Nordic countries, and *vice versa*. In the face of the Swedish surveillance legislation this communication is as threatened by the risk of interception as any other communication. Needless to say,

[7] See, for instance, *Goodwin v. The United Kindom*, ECHR judgment 27.03.96 and *Weber and Saravia v. Germany*, ECHR decision 29.06.06

this is more than likely to have a seriously chilling effect on all such communication. This is especially critical with regard to communication which pertains to government-critical ideas or information. If a potential source for the press knows that he or she, by communicating cross-border with a journalist, is running the risk of the authorities intercepting that communication, the source might very well abstain from communicating all together. In turn the press is cut off from potentially vital sources in its role as public watchdog, and the public is denied information which it has the right to receive.

35. According to the jurisprudence of the Court, the question of whether strategic surveillance of communications between journalists and their sources constitutes a proportional interference according to Article 10 must depend on whether the legislation contains safeguards that can be considered adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum. Consequently, the fact that the most central safeguards contained in the Swedish legislation are not available to foreign journalist, indicates that the legislation must be considered a disproportional interference in foreign journalists' right to protect their sources.

36. Therefore, and in conclusion, the Swedish surveillance legislation strikes directly at the core of two of the main pillars of a democratic society; the right to respect for privacy and correspondence and the freedom of expression, in addition to generally undermining the Rule of Law. In neither respect can this interference be said to satisfy the requirements regarding quality of domestic law or the necessity-test, as set out in the Convention.

## VI LIST OF ATTACHMENTS

37. The following documents, referred to in text and foot notes above, are enclosed as attachments, in numerical order:

    1) ICJ-Norway's Articles of Association
    2) "Notat om "FRA-loven" og ruting av elektronisk kommunikasjon via Sverige", Post- og teletilsynet, November 2008
    3) "Signalspaningslagen", Regeringskanseliet, September/October 2008

***

Oslo, February 11th 2009