European Court of Human Rights: Centrum för Rättvisa v. Sweden

IRIS 2018-8:1/3

Dirk Voorhoof
Human Rights Centre, Ghent University and Legal Human Academy

According to the European Court of Human Rights (ECtHR), the Swedish law permitting the bulk interception of electronic signals in Sweden for foreign intelligence purposes does not violate the right to privacy and correspondence under Article 8 of the European Convention on Human Rights (ECHR). The ECtHR reached this conclusion after a Swedish human rights not-for-profit organisation, Centrum för Rättvisa ("the Centrum"), lodged a complaint with the Strasbourg Court, alleging that Swedish legislation and practice in the field of signals intelligence violated and continued to violate its privacy rights under Article 8 of the ECHR.

"Signals intelligence" can be defined as the interception, processing, analysis and reporting of intelligence derived from electronic signals. These signals may be converted to text, images and sound. In Sweden, signals intelligence is conducted by the National Defence Radio Establishment (Försvarets radioanstalt - "the FRA") and regulated by the Signals Intelligence Act. Owing to the nature of its function as a non-governmental organisation scrutinising the activities of state actors, the Centrum argued that there is a risk that those of its communication activities carried out by means of mobile telephones and mobile broadband had been or could be intercepted and examined by way of signals intelligence. The Centrum has not brought any domestic proceedings, contending that there was or is no effective remedy for its Convention complaints.

The ECtHR considered that the contested legislation regulating signals intelligence establishes a system of secret surveillance that potentially affects all users of, for example, mobile telephone services and the Internet, without their being notified of such surveillance. And, because no domestic legal remedies provide detailed grounds in response to a complainant who suspects that his or her communications have been intercepted.

In these circumstances, the ECtHR accepted that an examination of the Swedish legislation in abstracto is justified. It emphasised that, especially where a power vested in the executive is exercised in secret, the risk of arbitrariness is evident; therefore it is essential to have clear, detailed rules on the interception of telephone and Internet communications, especially as the relevant technology available is continually becoming more sophisticated. In view of the risk that a

system of secret surveillance set up to protect national security may undermine, or even destroy, democracy under the cloak of defending it, the ECtHR must be satisfied that there are adequate and effective guarantees against abuse. Any assessment of this question must depend on all the circumstances of the case, such as the nature, scope and duration of possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.

As the ECtHR considered that it is clear that the Swedish law permitting signals intelligence pursues legitimate aims in the interest of national security, it remained to be ascertained whether the law is accessible and contains adequate and effective safeguards and guarantees to be considered "foreseeable" and "necessary in a democratic society".

The ECtHR found that the Swedish law indicates the scope for mandating and performing signals intelligence conferred on the competent authorities and the manner of the exercise thereof sufficient clarity, and it was satisfied that there are safeguards in place which adequately regulate the duration, renewal and cancellation of interception measures. Most importantly, permission to undertake interception measures have to be authorised by court order, and only after a detailed examination; it was only permitted in respect of communications crossing the Swedish border and not within Sweden itself; such measures could only last for a maximum of six months; and any renewal required a court review. The ECtHR found that the provisions and procedures regulating the system of prior court authorisation, on the whole, provide important guarantees against abuse. Examining the legislation on storing, accessing, examining, using and destroying intercepted data, the ECtHR was also satisfied that it provides adequate safeguards against the abusive treatment of personal data and thus serves to protect individuals' personal integrity. Although a certain lack of specification in the provisions regulating the communication of personal data to other states and international organisations gives some cause for concern with respect to the possible abuse of the rights of individuals, on the whole, the ECtHR considered that the supervisory elements in place sufficiently counterbalance these regulatory shortcomings. Lastly, the ECtHR agreed with the Swedish Government that the lack of notification of surveillance measures is compensated for by the fact that there are a number of complaint mechanisms available - in particular those that could be exercised via the Data Protection Authority, the Parliamentary Ombudsmen and the Chancellor of Justice. However, the ECtHR observed that the Swedish remedies available in relation to complaints relating to secret surveillance do not include recourse to a court, nor do they offer other effective remedies.

Furthermore, individuals are not informed of whether their communications have actually been intercepted, and neither are they generally given reasoned

decisions. However, it ruled that the total number of available remedies, although not providing a full and public response to the objections raised by the Centrum, must be considered sufficient in the present context, which concerns an abstract challenge to the signals intelligence regime itself and does not concern a complaint against a particular intelligence measure. In reaching this conclusion, the Court attaches importance to the earlier stages of supervision of the signals intelligence regime, including the detailed judicial examination by the Foreign Intelligence Court of the FRA's requests for permits to conduct signals intelligence and the extensive and partly public supervision by several bodies (in particular the Foreign Intelligence Inspectorate).

Although the ECtHR stressed that it is mindful of the potentially harmful effects that the operation of a signals intelligence scheme may have on the protection of privacy, it acknowledged the importance for national security operations of a system such as the Swedish one, having regard to the present-day threats being posed by global terrorism and serious cross-border crime, as well as the increased sophistication of communications technology. The ECtHR was of the opinion that the Swedish system on signals intelligence reveals no significant shortcomings in its structure and operation and that it provides adequate and sufficient guarantees against arbitrariness and the risk of abuse. It therefore ruled that there had been no violation of Article 8 of the ECHR.

Judgment by the European Court of Human Rights, Third Section, case of Centrum för Rättvisa v. Sweden, Application no. 35252/08, 19 June 2018

https://hudoc.echr.coe.int/eng?i=001-183863