European Court of Human Rights: Big Brother Watch and Others v. the United Kingdom

IRIS 2018-10:1/1

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

A short time after the judgment in Centrum för Rättvisa v. Sweden (see IRIS 2018-8/3), the European Court of Human Rights (ECtHR) has delivered a new judgment on the bulk interception of communications and intelligence sharing. This time, the ECtHR has found several violations of the European Convention on Human Rights (ECHR) in the United Kingdom's regime for bulk interception of communications, including a violation of the right of journalists to protect their sources. It is important, however, to underscore that the UK has updated its surveillance rules under new legislation, the Investigatory Powers Act 2016 (IPA 2016), which has not yet fully come into force. The ECtHR did not examine the new legislation in its judgment of 13 September 2018.

The judgment in the case of Big Brother Watch and Others v. the United Kingdom deals with a complex set of statutory laws, codes of conduct, procedures and monitoring instruments on the bulk interception of communications, intelligence sharing and requesting data from communications service providers. The judgment counts 204 pages, including separate opinions, though with a very helpful structure produced by the ECtHR itself, accompanied by an instructive press release and even an explanatory Q&A-document as "a tool for the press".

The applications with the Strasbourg Court were lodged by organisations and individuals who actively campaign on issues of civil liberties; by a newsgathering organisation; and by a journalist complaining about the scope and magnitude of the electronic surveillance programmes operated by the UK Government. The applications were lodged after Edward Snowden, a former US National Security Agency (NSA) contractor, revealed the existence of surveillance and intelligence-sharing programmes operated by the intelligence services of the United States and the UK. The applicants believed that the nature of their activities meant that their electronic communications and/or communications data were likely to have been intercepted or obtained by the UK intelligence services.

The ECtHR expressly recognised the severity of the threats currently facing many contracting states, including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime. It also recognised that advancements in technology have made it easier for terrorists and criminals to evade detection on the Internet.

© European Audiovisual Observatory (Council of Europe) 2024

It therefore held that states should enjoy broad discretion in choosing how best to protect national security. Consequently, a state may operate a bulk interception regime if it considers it necessary in the interests of national security. However, the ECtHR does not ignore the fact that surveillance regimes have the potential to be abused, with serious consequences for individual privacy. In order to minimise this risk, the ECtHR reiterated that six minimum safeguards must exist. These safeguards are that the national law must clearly indicate: the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed.

With regard to the bulk interception of communications, the ECtHR came to the conclusion that the UK intelligence services take their Convention obligations seriously and do not abuse their powers; however, it considered that there was inadequate independent oversight of the selection and search processes involved in the operation, in particular when it came to selecting the Internet bearers for interception and choosing the selectors and search criteria used to filter and select intercepted communications for examination. Furthermore, there were no real safeguards applicable to the selection of related communications data for examination, even though this data could reveal a great deal about a person's habits and contacts. The ECtHR also referred to a wide range of possibilities for public bodies to request access to communications data from communications companies in various ill-defined circumstances. According to the ECtHR, the legal regime in the UK allowing access to data held by communications service providers was not limited to the purpose of combatting "serious crime", and there were no sufficient guarantees to prior review by a court or independent administrative body. Therefore, the ECtHR came to the conclusion that Article 8 of the ECHR was being breached.

On the issue of requesting intelligence from foreign intelligence agencies, the ECtHR found that the regulatory provisions in the UK were formulated with sufficient clarity in the domestic law and in the relevant code of practice. As there was no evidence of any significant shortcomings in the application and operation of the regime, or evidence of any abuse, the ECtHR found no violation of Article 8 of the ECHR on this matter.

The specific complaint with regard to Article 10 of the ECHR by the Bureau of Investigative Journalism and the journalist Alice Ross, supported by third party interventions submitted by the National Union of Journalists, the International Federation of Journalists, the Media Lawyers' Association and the Helsinki Foundation for Human Rights, led to the finding that the bulk surveillance regimes in the UK did not provide sufficient protection for journalistic sources or

© European Audiovisual Observatory (Council of Europe) 2024

confidential journalistic material. The ECtHR reiterated that the protection of journalistic sources is one of the cornerstones of freedom of the press, and that interference cannot be compatible with Article 10 of the ECHR unless it is justified by an overriding requirement in the public interest. Carrying out searches at a journalist's home and workplace with a view to uncovering his or her sources, even if unproductive, constitutes a more drastic measure than an order to divulge the source's identity, since investigators who raid a journalist's workplace have access to all the documentation held by the journalist. Therefore special consideration is to be given to the interception of communications that involve confidential journalistic material and confidential personal information. The ECtHR expressed particular concern about the absence of any published safeguards in the UK relating both to the circumstances in which confidential journalistic material could be selected intentionally for examination, and to the protection of confidentiality where it had been selected, either intentionally or otherwise, for examination. In view of the potential chilling effect that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press and, in the absence of any published arrangements limiting the intelligence services' ability to search and examine such material other than where "it was justified by an overriding requirement in the public interest", the ECtHR found the bulk interception regime in violation of Article 10 of the ECHR. With regard to the requests for data from communications service providers, yet again, the ECtHR did not find sufficient guarantees to protect journalists' sources: the relevant safeguards do not apply in every case where there is a request for a journalist's communications data, or where collateral intrusion is likely. In addition, there are no special provisions restricting access for the purpose of combatting "serious crime". As a consequence, the ECtHR also found a violation of journalists' rights under Article 10 of the ECHR in respect of the regime for data requests from communication service providers.

Judgment by the European Court of Human Rights, First Section, case of Big Brother Watch and Others v. the United Kingdom, Application Nos. 58170/13, 62322/14 and 24960/15, 13 September 2018

http://hudoc.echr.coe.int/eng?i=001-186048

© European Audiovisual Observatory (Council of Europe) 2024

© European Audiovisual Observatory (Council of Europe) 2024