September 2018
This Factsheet does not bind the Court and is not exhaustive

Mass surveillance

Article 8 (right to respect for private and family life, home and correspondence) of the European Convention on Human Rights provides that:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

In order to determine whether the interference by the authorities with the applicants' private life or correspondence was necessary in a democratic society and a fair balance was struck between the different interests involved, the European Court of Human Rights examines whether the interference was in accordance with the law, pursued a legitimate aim or aims and was proportionate to the aim(s) pursued.

Klass and Others v. Germany

6 September 1978 (judgment)

In this case the applicants, five German lawyers, complained in particular about legislation in Germany empowering the authorities to monitor their correspondence and telephone communications without obliging the authorities to inform them subsequently of the measures taken against them.

The European Court of Human Rights held that there had been **no violation of Article 8** of the European Convention on Human Rights, finding that the German legislature was justified to consider the interference resulting from the contested legislation with the exercise of the right guaranteed by Article 8 as being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime. The Court observed in particular that powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions. Noting, however, that democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction, the Court considered that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications was, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.

Weber and Saravia v. Germany

29 June 2006 (decision on the admissibility)

The applicants – the first one was a freelance journalist and the second one was taking telephone messages for the first applicant and passed them on to her – claimed in particular that certain provisions of the 1994 Fight against Crime Act amending the 1968 Act on Restrictions on the Secrecy of Mail, Post and Telecommunications ("the G 10

Act")[1], in their versions as interpreted and modified by the Federal Constitutional Court in a judgment of 14 July 1999, violated their right to respect for their private life and their correspondence

The Court declared the applicant's complaint **inadmissible** as being manifestly ill-founded. Having regard to all the impugned provisions of the amended G 10 Act in their legislative context, it found that there existed adequate and effective guarantees against abuses of the State's strategic monitoring powers. The Court was therefore satisfied that Germany, within its fairly wide margin of appreciation in that sphere, was entitled to consider the interferences with the secrecy of telecommunications resulting from the impugned provisions to have been necessary in a democratic society in the interests of national security and for the prevention of crime.

Liberty and Others v. the United Kingdom

1 July 2008 (judgment)

The applicants, a British and two Irish civil liberties' organisations, alleged that, between 1990 and 1997, their telephone, facsimile, e-mail and data communications, including legally privileged and confidential information, were intercepted by an Electronic Test Facility operated by the British Ministry of Defence. They had lodged complaints with the Interception of Communications Tribunal, the Director of Public Prosecutions and the Investigatory Powers Tribunal to challenge the lawfulness of the alleged interception of their communications, but to no avail.

The Court held that there had been a **violation of Article 8** of the Convention. It did not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the authorities to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law".

Kennedy v. the United Kingdom

18 May 2010 (judgment)

Suspecting police interception of his communications after he had started a small business, the applicant complained to the Investigatory Powers Tribunal (IPT). He was eventually informed in 2005 that no determination had been made in his favour in respect of his complaints. This meant either that his communications had not been intercepted or that the IPT considered any interception to be lawful. No further information was provided by the IPT. The applicant complained about the alleged interception of his communications.

The Court held that there had been **no violation of Article 8** of the Convention, finding that UK law on interception of internal communications together with the clarifications brought by the publication of a Code of Practice indicated with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of data collected. Moreover, there was no evidence of any significant shortcomings in the application and operation of the surveillance regime. Therefore, and having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, in so far

[1]. The G 10 Act was amended to accommodate the so-called strategic monitoring of telecommunications, that is, collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences. The changes notably concerned the extension of the powers of the Federal Intelligence Service with regard to the recording of telecommunications in the course of strategic monitoring, as well as the use of personal data obtained thereby and their transmission to other authorities.

as they might have been applied to the applicant, had been justified under Article 8 of the Convention.

Roman Zakharov v. Russia

4 December 2015 (judgment – Grand Chamber)

This case concerned the system of secret interception of mobile telephone communications in Russia. The applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law-enforcement agencies to carry out operational-search activities and that, without sufficient safeguards under Russian law, this permitted blanket interception of communications.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications. In particular, the Court found shortcomings in the legal framework in the following areas: the circumstances in which public authorities in Russia are empowered to resort to secret surveillance measures; the duration of such measures, notably the circumstances in which they should be discontinued; the procedures for authorising interception as well as for storing and destroying the intercepted data; the supervision of the interception. Moreover, the effectiveness of the remedies available to challenge interception of communications was undermined by the fact that they were available only to persons who were able to submit proof of interception and that obtaining such proof was impossible in the absence of any notification system or possibility of access to information about interception.

See also, concerning secret surveillance measures in the context of criminal proceedings: **Akhlyustin v. Russia**, **Zubkov and Others v. Russia**, **Moskalev v. Russia** and **Konstantin Moskalev v. Russia**, judgments of 7 November 2017.

Szabó and Vissy v. Hungary

12 January 2016 (judgment)

This case concerned Hungarian legislation on secret anti-terrorist surveillance introduced in 2011. The applicants complained in particular that they could potentially be subjected to unjustified and disproportionately intrusive measures within the Hungarian legal framework on secret surveillance for national security purposes (namely, "section 7/E (3) surveillance"). They notably alleged that this legal framework was prone to abuse, notably for want of judicial control.

In this case the Court held that there had been a **violation of Article 8** of the Convention. It accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents. However, the Court was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. Notably, the scope of the measures could include virtually anyone in Hungary, with new technologies enabling the Government to intercept masses of data easily concerning even persons outside the original range of operation. Furthermore, the ordering of such measures was taking place entirely within the realm of the executive and without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place. The Court further held that there had been **no violation of Article 13** (right to an effective remedy) of the Convention **taken together with Article 8**, reiterating that Article 13 could not be interpreted as requiring a remedy against the state of domestic law.

Centrum För Rättvisa v. Sweden

19 June 2018 (judgment)[2]

This case concerned a complaint brought by a public interest law firm alleging that legislation permitting the bulk interception of electronic signals in Sweden for foreign intelligence purposes breached its privacy rights.

The Court held that there had been **no violation of Article 8** of the Convention in the present case. It considered in particular that the relevant legislation amounted to a system of secret surveillance that potentially affected all users of mobile telephones and the Internet, without their being notified. Also, there was no domestic remedy providing detailed grounds in response to a complainant who suspected that his or her communications had been intercepted. On that basis, the Court found it justified to examine the legislation in the abstract. In this regard, the Court noted that, athough there were some areas for improvement, overall the Swedish system of bulk interception provided adequate and sufficient guarantees against arbitrariness and the risk of abuse. In particular, the scope of the signals intelligence measures and the treatment of intercepted data were clearly defined in law, permission for interception had to be by court order after a detailed examination, it was only permitted for communications crossing the Swedish border and not within Sweden itself, it could only be for a maximum of six months, and any renewal required a review. Furthermore, there were several independent bodies, in particular an inspectorate, tasked with the supervision and review of the system. Lastly, the lack of notification of surveillance measures was compensated for by the fact that there were a number of complaint mechanisms available, in particular via the inspectorate, the Parliamentary Ombudsmen and the Chancellor of Justice. When coming to that conclusion, the Court took into account the State's discretionary powers in protecting national security, especially given the present-day threats of global terrorism and serious cross-border crime.

Big Brother Watch and Others v. the United Kingdom (nos. 58170/13, 62322/14 and 24960/15)

13 September 2018 (judgment) [3]

These applications were lodged after revelations by Edward Snowden (former contractor with the US National Security Agency) about programmes of surveillance and intelligence sharing between the USA and the United Kingdom. The case concerned complaints by journalists and civil liberties organisations about three types of surveillance: the bulk interception of communications; intelligence sharing with foreign governments; and the obtaining of communications data from service providers.

The Court held that the bulk interception regime **violated Article 8** (right to respect for private and family life) of the Convention as there was insufficient oversight both of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, and the safeguards governing the selection of "related communications data" for examination were inadequate. In reaching this conclusion, the Court found that the operation of a bulk interception regime did not in and of itself violate the Convention, but noted that such a regime had to respect criteria set down in its case-law. The Court also held that the regime for obtaining communications data from communications service providers **violated Article 8** as it was not in accordance with the law; and that both the bulk interception regime and the regime for obtaining communications data from communications service providers **violated Article 10** (freedom of expression) of the Convention as there were insufficient safeguards in respect of confidential journalistic material. It further found that the regime for sharing intelligence with foreign governments **did not violate either Article 8 or Article 10** of the Convention. Lastly, the Court **rejected complaints** made by the third set of applicants under **Article 6** (right to a fair trial) of the Convention, about the

2. This judgment will become final in the circumstances set out in Article 44 § 2 (final judgments) of the European Convention on Human Rights.
3. This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention.

domestic procedure for challenging secret surveillance measures, **and under Article 14** (prohibition of discrimination) of the Convention.

Pending applications

Tretter and Others v. Austria (no. 3599/10)

Application communicated to the Austrian Government on 6 May 2013

This case concerns the amendments of the Police Powers Act, which entered into force in January 2008 and extended the powers of the police authorities to collect and process personal data.

The Court gave notice of the application to the Austrian Government and put questions to the parties under Articles 8 (right to respect for private life and correspondence), 10 (freedom of expression) and 34 (right of individual petition) of the Convention.

Similar application pending: **Ringler v. Austria (no. 2309/10)**, communicated to the Austrian Government on 6 May 2013.

Association confraternelle de la presse judiciaire v. France et 11 autres requêtes (nos. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15)

Applications communicated to the French Government on 26 April 2017

These applications, which were lodged by lawyers and journalists, as well as legal persons connected with these professions, concern the French Intelligence Act of 24 July 2015.

The Court gave notice of the applications to the French Government and put questions to the parties under Articles 8 (right to respect for private life and correspondence), 10 (freedom of expression) and 13 (right to an effective remedy) of the Convention.

Similar applications pending: **Follorou v. France (no. 30635/17) and Johannes v. France (no. 30636/17)**, communicated to the French Government on 4 July 2017.

Further reading

See in particular:

- **"Personal data protection"**, factsheet prepared by the Court's Press Unit
- **National security and case-law of the European Court of Human Rights**, report prepared by the Research Division of the Court, November 2013 *(available in French only)*

Media Contact:
Tel.: +33 (0)3 90 21 42 08