June 2024
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 complained of 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.

Breyer v. Germany

30 January 2020 (judgment)

In accordance with 2004 amendments to the German Telecommunications Act companies had to collect and store the personal details of all their customers, including users of pre-paid SIM cards, which had not previously been required. The applicants, civil liberties activists and critics of State surveillance, were users of such cards and therefore had to register their personal details, such as their telephone numbers, date of birth, and their name and address, with their service providers. They complained about the storage of their personal data as users of pre-paid SIM cards.

The Court held that there had been **no violation of Article 8** of the Convention, finding that, overall, Germany had not overstepped the limits of its discretion ("margin of appreciation") it had in applying the law concerned, when choosing the means to achieve the legitimate aims of protecting national security and fighting crime, and that the storage of the applicants' personal data had been proportionate and "necessary in a democratic society". There had thus been no violation of the Convention. The Court considered in particular that collecting the applicants' names and addresses as users of pre-paid SIM cards had amounted to a limited interference with their rights. It noted, however, that the law in question had additional safeguards while people could also turn to independent data supervision bodies to review authorities' data requests and seek legal redress if necessary.

Privacy International and Others v. the United Kingdom

7 July 2020 (decision on the admissibility)

The applicants – an NGO registered in London, an Internet service provider registered in London, an association of "hacktivists" registered in Germany, two companies registered in the United States providing Internet services and communications services respectively, and an Internet service provider registered in South Korea – believed that their equipment had been subject to interference, colloquially known as "hacking", over an undefined period by the United Kingdom Government Communications Headquarters and/or the Secret Intelligence Service. They complained in particular that the power under Section 7 of the Intelligence Services Act[2] was not in accordance with the law, that it contained no requirement for judicial authorisation, that there was no information in the public domain about how it might be used to authorise Equipment Interference, and that there was no requirement for filtering to exclude irrelevant material. They added that the Investigatory Powers Tribunal did not provide an effective remedy as it did not rule on the Section 7 regime in the domestic litigation.

The Court declared the applicants' complaints under Article 8, Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention **inadmissible**, finding that, in the circumstances of the case, the applicants had not provided the domestic courts, notably the Investigatory Powers Tribunal, with the opportunity which is in principle intended by Article 35 (admissibility criteria) of the Convention to be afforded to a Contracting State, namely the opportunity of addressing, and thereby preventing or putting right, the particular Convention violation alleged against it. The Court noted in particular the general arguments advanced by the applicants and also underlined in the interventions of the third parties that the surveillance complained of was particularly intrusive and that there was a need for safeguards in this domain. In that respect, it recalled the importance of examining compliance with the principles of Article 8 of the Convention where the powers vested in the State are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated. However, that importance reinforced in the context of exhaustion of domestic remedies the need to provide the domestic courts with the possibility to rule on such matters where they have the potential to do so.

[2]. Section 7 of the Intelligence Services Act 1994 ("the ISA") allows the Secretary of State to authorise a person to undertake (and to exempt them from liability for) an act outside the British Islands in relation to which they would be liable if it were done in the United Kingdom.

Big Brother Watch and Others v. the United Kingdom

25 May 2021 (judgment – Grand Chamber)

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 human-rights organisations in regard to three different surveillance regimes: (1) the bulk interception of communications; (2) the receipt of intercept material from foreign governments and intelligence agencies; (3) the obtaining of communications data from communication service providers[3].

The Grand Chamber held: unanimously, that there had been a **violation of Article 8** of the Convention in respect of the bulk intercept regime; unanimously, that there had been a **violation of Article 8** in respect of the regime for obtaining communications data from communication service providers; by twelve votes to five, that there had been **no violation of Article 8** in respect of the United Kingdom's regime for requesting intercepted material from foreign Governments and intelligence agencies; unanimously, that there had been a **violation of Article 10** (freedom of expression) of the Convention, concerning both the bulk interception regime and the regime for obtaining communications data from communication service providers; and, by twelve votes to fives, that there had been **no violation of Article 10** in respect of the regime for requesting intercepted material from foreign Governments and intelligence agencies. The Court considered in particular that, owing to the multitude of threats States face in modern society, operating a bulk interception regime did not in and of itself violate the Convention. However, such a regime had to be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation were being defined; and that the operation should be subject to supervision and independent *ex post facto* review. Having regard to the bulk interception regime operated in the UK, the Court identified the following deficiencies: bulk interception had been authorised by the Secretary of State, and not by a body independent of the executive; categories of search terms defining the kinds of communications that would become liable for examination had not been included in the application for a warrant; and search terms linked to an individual (that is to say specific identifiers such as an email address) had not been subject to prior internal authorisation. The Court also found that the bulk interception regime had not contained sufficient protections for confidential journalistic material. The regime for obtaining communications data from communication service providers was also found to have not been in accordance with the law. However, the Court held that the regime by which the UK could request intelligence from foreign governments and/or intelligence agencies had had sufficient safeguards in place to protect against abuse and to ensure that UK authorities had not used such requests as a means of circumventing their duties under domestic law and the Convention.

Centrum För Rättvisa v. Sweden

25 May 2021 (judgment – Grand Chamber)

This case concerned the alleged risk that the applicant foundation's communications had been or would be intercepted and examined by way of signals intelligence, as it communicated on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax, often on sensitive matters.

The Grand Chamber held, by fifteen votes to two, that there had been a **violation of Article 8** of the Convention. It found, in particular, that although the main features of

[3]. At the relevant time, the regime for bulk interception and obtaining communications data from communication service providers had a statutory basis in the Regulation of Investigatory Powers Act 2000. This had since been replaced by the Investigatory Powers Act 2016. The findings of the Grand Chamber relate solely to the provisions of the 2000 Act, which had been the legal framework in force at the time the events complained of had taken place.

the Swedish bulk interception regime met the Convention requirements on quality of the law, the regime nevertheless suffered from three defects: the absence of a clear rule on destroying intercepted material which did not contain personal data; the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration was given to the privacy interests of individuals; and the absence of an effective *ex post facto* review. As a result of these deficiencies, the system did not meet the requirement of "end-to-end" safeguards, it overstepped the margin of appreciation left to the respondent State in that regard, and overall did not guard against the risk of arbitrariness and abuse.

Ekimdzhiev and Others v. Bulgaria

11 January 2022 (judgment)

The applicants – two lawyers and two non-governmental organisations – alleged, in particular, that under the system of secret surveillance in Bulgaria the communications of anyone in the country could be intercepted, and that under the system of retention and subsequent accessing of communications data the communications data of anyone in the country could be accessed by the authorities. They submitted that the laws governing those two matters, as applied in practice, did not provide sufficient safeguards against arbitrary or abusive secret surveillance and accessing of communications data.

The Court held that there had been a **violation of Article 8** of the Convention, in respect of secret surveillance, finding that the relevant legislation governing secret surveillance, especially as applied in practice, did not meet the quality-of-law requirement of the Convention and was unable to keep surveillance to only that which was necessary. It also held that there had been a **violation of Article 8**, in respect of retention and accessing of communication data, finding that, as the laws governing retention and accessing communications data did not meet the quality-of-law requirement of the Convention, they were incapable of limiting such retention and accessing to what was necessary. Moreover, in this judgment, the Court emphasised that pursuant to **Article 46** (binding force and execution of judgments) of the Convention, a State party had to make the necessary changes to domestic law to end the violation and restore as far as possible the situation which would have obtained if it had not taken place, and to ensure its laws were compatible with the Convention. In the present case, the measures would have to supplement those which the Bulgarian authorities had already taken to implement the judgment *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* of 28 June 2007.

Haščák v. Slovakia

23 June 2022 (judgment)

This case concerned a surveillance operation ("the Gorilla operation") carried out in 2005 and 2006 by the Slovak Intelligence Service (SIS) and the intelligence material obtained by it. The applicant – a prominent businessman associated with an influential finance group and a business partner of the applicant in the case of Zoltán Varga v. Slovakia (judgment of 20 July 2021) – complained, in particular, that there had been a lack of effective supervision and review of the implementation of two surveillance warrants issued by the Bratislava Regional Court in the mid-2000s, that the applicable framework provided no protection to individuals randomly affected by surveillance measures, and that the internal rules applicable to the retention of intelligence material were inadequate.

The Court held that there had been a **violation of Article 8** of the Convention concerning the implementation of the two warrants and the retention of the analytical material. It firstly stated that to a significant extent, the applicant's complaints under Article 8 were identical and arose from an identical factual and procedural background to that examined in the case of *Zoltán Varga*. It therefore applied that case-law to the present case. While there had been a basis in law, the Court observed in particular

that the operation had had numerous deficiencies, some of which had been recognised at the domestic level in response to complaints and actions of Mr Varga. Although the domestic courts made no such findings in the individual case of the applicant, they were relevant to the assessment of his case. The Court reiterated that, as in *Zoltán Varga*, when implementing the surveillance warrants the SIS had practically enjoyed discretion amounting to unfettered power, which had not been accompanied by a measure of protection against arbitrary interference, as required by the rule of law. Furthermore, that situation had been aggravated by the uncontested fact that the applicant had not himself been the target of the surveillance under the first of the two warrants, in the light of his unchallenged argument that the law provided no protection to persons randomly affected by surveillance measures, and by the fundamental uncertainty around the practical and procedural status of the audio recording retrieved in 2018, presumably of SIS provenance. The Court lastly noted that it had previously held in *Zoltán Varga* that the storing of the analytical material obtained in the surveillance operation had been subject to confidential rules with no external oversight. The retention had therefore not been in accordance with the law. The Court ruled that that also applied in the present case.

Pietrzak and Bychawska-Siniarska and Others v. Poland

28 May 2024 (judgment[4])

This case concerned a complaint by five Polish nationals about Polish legislation authorising a secret-surveillance regime covering both operational control and the retention of telecommunications, postal and digital communications data ("communications data") for possible future use by the relevant national authorities. In particular, they alleged that there was no remedy available under domestic law allowing persons who believed that they had been subjected to secret surveillance to complain about that fact and to have its lawfulness reviewed.

The Court held that there had been three **violations of Article 8** of the Convention in respect of the complaints concerning the operational-control regime, the retention of communications data for potential use by the relevant national authorities, and the secret-surveillance regime under the Anti-Terrorism Act. Firstly, given the secret nature and wide scope of the measures provided for by the Polish legislation and the lack of effective review by which persons who believed that they had been subjected to surveillance could challenge this alleged surveillance, the Court found it appropriate to examine the legislation at issue in abstracto. It considered that the applicants could claim to be the victims of a violation of the Convention, and that the mere existence of the relevant legislation constituted in itself an interference with their Article 8 rights. The Court then held that all the shortcomings identified by it in the operational-control regime led to a conclusion that the national legislation did not provide sufficient safeguards against excessive recourse to surveillance and undue interference with individuals' private life; the absence of such guarantees was not sufficiently counterbalanced by the current mechanism for judicial review. In its view, the national operational-control regime, taken as a whole, did not comply with the requirements of Article 8. It further considered that the national legislation, under which information and communication technologies ("ICT") providers were required to retain communications data in a general and indiscriminate manner for possible future use by the relevant national authorities, was insufficient to ensure that the interference with the applicants' right to respect for their private life was limited to what was "necessary in a democratic society". Lastly, the Court concluded that the secret-surveillance provisions in the Anti-Terrorism Act also failed to satisfy the requirements of Article 8 of the Convention, noting, among other points, that neither the imposition of secret surveillance nor its application in the initial three-month period were subject to any review by a body that

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

was independent and did not include employees of the service conducting that surveillance.

See also the following decisions:

Ringler v. Austria

12 May 2020 (Committee – decision on the admissibility)

Tretter and Others v. Austria

29 September 2020 (Committee – decision on the admissibility)

Pending applications

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.

A.L. v. France (no. 44715/20) and E.J. v. France (no. 47930/21)

Applications communicated to the French Government on 8 December 2021

These applications concern in particular the infiltration by the French authorities of the encrypted communication network "EncroChat" and the capture, copying and analysis of data stored and exchanged with the devices connected to this network.

The Court gave notice of the applications to the French Government and put questions to the parties under Articles 6 § 1 (right to a fair trial), 8 (right to respect for private life and correspondence), 13 (right to an effective remedy), 34 (right of individual application) and 35 (admissibility criteria) of the Convention.

Further reading

See in particular:

- ECHR Knowledge Sharing platform (ECHR-KS), Data protection

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