Thematic factsheet[1]
Update: June 2018

MASS SURVEILLANCE

The highly complex forms of terrorism require States to take effective measures to defend themselves, including mass monitoring of communications. Unlike "targeted" surveillance (covert collection of conversations, telecommunications and metadata by technical means – "bugging"), "strategic" surveillance (or mass surveillance) does not necessarily start with a suspicion against a particular person or persons. It has a proactive element, aimed at identifying a danger rather than investigating a known threat. Herein lay both the value it can have for security operations, and the risks it can pose for individual rights.

Nevertheless, Member States do not have unlimited powers in this area. Mass surveillance of citizens is tolerable under the Convention only if it is strictly necessary for safeguarding democratic institutions. Taking into account considerable potential to infringe fundamental rights to privacy and to freedom of expression enshrined by the Convention, Member States must ensure that the development of surveillance methods resulting in mass data collection is accompanied by the simultaneous development of legal safeguards securing respect for citizens' human rights.

According to the case-law of the European Court of Human Rights, it would be counter to governments' efforts to keep terrorism at bay if the terrorist threat were substituted with a perceived threat of unfettered executive power intruding into citizens' private lives. It is of the utmost importance that the domestic legislation authorizing far-reaching surveillance techniques and prerogatives provides for adequate and sufficient safeguards in order to minimize the risks for the freedom of expression and the right to privacy which the "indiscriminate capturing of vast amounts of communications" enables. The standards related to targeted surveillance identified in the case-law of the Court have therefore to be adapted to apply to strategic surveillance.

I. European Court of Human Rights' relevant case-law

- ***Szabó and Vissy v. Hungary*** - no. 37138/14: Hungarian legislation on secret anti-terrorist surveillance through new technologies enabling to intercept masses of data: Judgment 12.1.2016: **violation**
- ***Liberty and Others v. United Kingdom*** - no. 58243/00: Interception by the Ministry of Defence of the external communications of civil liberties organisations on the basis of a warrant issued under wide discretionary powers : Judgment 1.07.2008: **violation**
- ***Weber and Saravia v. Germany*** - no. 54934/00: Strategic monitoring of communications, in order to identify and avert serious dangers on the national territory,

[1] This document presents a non-exhaustive selection of the CoE instruments and of the European Court of Human Rights' relevant case-law. This information is not a legal assessment of the alerts and should not be treated or used as such.

such as an armed attack or terrorist attacks; appropriate safeguards regarding the media freedom. Decision 29.6.2006 : **inadmissible (manifestly ill founded)**

- ***Roman Zakharov v. Russia***: inadequate and ineffective guarantees against arbitrariness of the domestic system of covert interception of communications. Judgment 4.12.2015: **violation**
- ***Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*** : Secret service surveillance of journalists and order for them to surrender documents capable of identifying their sources. Judgment 22.11.2012 : **violation**
- ***Kennedy v. the United Kingdom***: Proportionality and suitable safeguards in the legislation on interception of internal communications. Judgment 18.05.2010 : **no violation**
- ***Klass et autres c. Allemagne*** : Lack of notification of the surveillance measures and alleged lack of legal remedy when such measures are terminated. Judgment 6.9.1978: **no violation**
- ***Mustafa Sezgin Tanrıkulu v. Turkey*** : Domestic court decision granting permission to national intelligence services, despite any legal basis, to intercept all domestic and international communications in Turkey for one and a half months with a view to identifying terrorist suspects. Judgment on 18 July 2017: **Violation**

Pending cases:

- *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (no. 62322/14)* and *10 Human Rights Organisations and Others v. the United Kingdom (no. 24960/15)* : Blanket interception, storage and exploitation of communication allegedly amounting to disproportionate interference with journalistic freedom of expression: Applications communicated to the UK Government on 5.01 and 24.11. 2015 : **pending**
- ***Association confraternelle de la presse judiciaire and others v. France*** - no. 49526/15: Protection of journalistic sources; compatibility the new French surveillance law ('loi no 2015-912 du 24 juillet 2015 relative au renseignement') with Articles 8 and 10 of the Convention. Communicated to the French Government on 26.4.2017: **pending**
- ***Big Brother Watch and Others v. the United Kingdom*** - no. 58170/13: Alleged indiscriminate capture and sharing of vast quantities of communication data by state security services. Communicated to the UK Government on 7.01.2014 : **pending**
- ***Hannes Tretter and Others against Austria:*** Extended powers given to the police authorities by the Police Powers Act allegedly interfered with the right to freedom of expression and had a "chilling effect" on all users of communication technologies such as mobile phones or e-mails. Communicated to the Austrian Government on 5.05.2013: **pending**

II. Other Council of Europe relevant resources

Venice Commission (European Commission for Democracy through Law)

- Report on the democratic oversight of the security services : June 2007
- Report on the democratic oversight of signals intelligence agencies : March 2015
- Poland: Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, (June 2016): Press release - DC109(2016)

Council of Europe Commissioner for Human Rights

- Issue Paper "Democratic and Effective Oversight of National Security Services" (2015)
- Human Rights at Risk when Secret Surveillance Spreads (2013)
- France: Statement "French Draft Law Seriously Infringes Human Rights", 13/04/2015; Letter To French Senate Https://Rm.Coe.Int/Ref/Commdh(2015)13 (20 May 2015)
- Poland: Commissioner's Press Release about his Visit to Poland :"Poland: Slow Down and Consult on Legislation to Avoid Human-Rights Backsliding" (2016)
- Germany: Shortcomings In the Oversight of German Intelligence and Security Services (2015)
- United Kingdom: **Memorandum on surveillance and oversight mechanisms in the United Kingdom** (May 2016)

Parliamentary Assembly

- Report on Mass Surveillance (2015)
- Resolution on Mass Surveillance 2045 (2015)
- Recommendation on Mass Surveillance 2067 (2015)

Committee of Ministers

- Reply to the Recommendation 2067 (2015) on Mass surveillance (Doc. 13911) 2015
- Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (2013)
- Recommendation no. R (87) 15 of the committee of ministers to member states regulating the use of personal data in the police sector (1987)
- Recommendation no. R (95) 4 of the committee of ministers to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (1995)

SUMMARY OF THE MOST RELEVANT CASE-LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS IN THE AREA OF MASS SURVEILLANCE

Hungarian legislation on secret anti-terrorist surveillance through new technologies enabling to intercept masses of data. Insufficient guarantees against abuse

Szabó and Vissy v. Hungary – no. 37138/14
Judgment 12.1.2016

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.

Interception by the Ministry of Defence of the external communications of civil-liberties organisations on the basis of a warrant issued under wide discretionary powers

Liberty and Others v. the United Kingdom – no. 58243/00
Judgment 1.7.2008

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".

Strategic monitoring of telecommunications. Sufficient safeguards regarding media freedom

Weber and Saravia v. Germany - no. 54934/00
Decision 29.6.2006

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, 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.

Article 8 - The Court declared the applicant's complaint **inadmissible**. 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. **Manifestly ill-founded.**

Article 10 – The first applicant submitted that the amended G 10 Act prejudiced the work of journalists investigating issues targeted by surveillance measures. She could no longer guarantee that information she received in the course of her journalistic activities remained confidential. In the Court's view, the threat of surveillance constitutes interference to her right, in her capacity as a journalist, to freedom of expression. The Court finds that this interference is prescribed by law and pursues a legitimate aim. As to its necessity in a democratic society, the Court notes that strategic surveillance was not aimed at monitoring journalists; surveillance measures were not directed at uncovering journalistic sources. It is true that the impugned provisions of the amended G 10 Act did not contain special rules safeguarding the protection of freedom of the press and, in particular, the non-disclosure of sources, once the authorities had become aware that they had intercepted a journalist's conversation. However, the Court observes that the impugned provisions contained numerous safeguards to keep the interference with the secrecy of telecommunications – and therefore with the freedom of the press – within the limits of what was necessary to achieve the legitimate aims pursued. In particular, the safeguards which ensured that data obtained were used only to prevent certain serious criminal offences must also be considered adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum. **Manifestly ill-founded.**

Lack of notification of the surveillance measures and alleged lack of legal remedy when such measures are terminated

Klass and Others v. Germany
Judgment 6 September 1978

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.

Proportionality and suitable safeguards in the legislation on interception of internal communications

Kennedy v. the United Kingdom
Judgment 18.05.2010

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

Inadequate and ineffective guarantees against arbitrariness of the domestic system of covert interception of communications

Roman Zakharov v. Russia
Judgment 4 December 2015

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.

Indiscriminate capture and sharing of vast quantities of communication data by state security services

Big Brother Watch and Others v. the United Kingdom – no. 58170/13

The applicants are three non-governmental organisations based in London and an academic based in Berlin, all of whom work internationally in the fields of privacy and freedom of expression. Their applications to the Court were triggered by media coverage, following the leak of information by Edward Snowden about the use by the United States of America and the United Kingdom of technologies permitting the indiscriminate capture of vast quantities of communication data and the sharing of such data between the two States.

The applicants allege that they are likely to have been the subject of generic surveillance by the UK Government Communications Head Quarters (GCHQ) and/or that the UK security services may have been in receipt of foreign intercept material relating to their electronic communications. They contend that the generic interception of external communications by GCHQ, merely on the basis that such communications have been transmitted by transatlantic fibre-optic cables, is an inherently disproportionate interference with the private lives of thousands, perhaps millions, of people. **Pending**

Blanket interception, storage and exploitation of communication allegedly amounting to disproportionate interference with journalistic freedom of expression

Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (no. 62322/14) and 10 Human Rights Organisations and Others v. the United Kingdom (no. 24960/15)

This cases concern the allegations of the applicants – the Bureau of Investigative Journalism and an investigative reporter who has worked for the Bureau – regarding the interception of both internet and telephone communications by government agencies in the United Kingdom, and, in particular, by the Government Communication Headquarters (GCHQ), as revealed by Edward Snowden, a former systems administrator with the United States National Security Agency (the NSA). The applicants mainly complain that the blanket interception, storage and exploitation of communication amount to disproportionate interference with journalistic freedom of expression. **Pending**

Compatibility the French surveillance law with the need to protect the journalistic sources

Association confraternelle de la presse judiciaire and others v. France - no. 49526/15

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. **Pending**