Thematic factsheet[1]
February 2016

MASS SURVEILLANCE

I. European Court of Human Rights' case law

- ***Szabó and Vissy v. Hungary*** - no. 37138/14: Hungarian legislation on secret anti-terrorist surveillance ; 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, such as an armed attack or terrorist attacks; safeguards regarding the media freedom. Decision 29.6.2006 : inadmissible
- ***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. Case communicated to the Austrian Government on 5.05.2013: pending
- ***Association confraternelle de la presse judiciaire and others v. France*** - no. 49526/15: Protection of journalistic sources ; compatibility with the French mass surveillance law and with Article 10 of the Convention. Lodged on 3.10.2015 and pending

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

II. Other Council of Europe relevant resources

➢ **European Commission for Democracy through Law (Venice Commission)**

- Report on the democratic oversight of the security services (Venice, 1-2 June 2007)
- Report on the democratic oversight of signals intelligence agencies (Venice, 7 April 2015)

➢ **Council of Europe Commissioner for Human Rights**

- CommHR 2015 "Issue Paper on Democratic and effective oversight of national security services"
- Human rights at risk when secret surveillance spreads (2013)
- "French Draft law seriously infringes human rights", *Le Monde*, 13.04.2015

➢ **Parliamentary Assembly**

- Report on Mass Surveillance. (Doc. 13734): 18.3.2015
- 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): 14.10. 2015
- Recommendation No. R (87) 15 of the Committee of Ministers to member States regulating the use of personal data in the police sector: 17.09.1987
- 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: 7.02.1995

➢ **Convention No°108 for the Protection of Individuals with regard to Automatic Processing of Personal Data**

APPENDIX

SUMMARY OF THE MOST RELEVANT CASE LAW IN THE AREA OF MASS SURVEILLANCE

Hungarian legislation on secret anti-terrorist surveillance. Absence of sufficient guarantees against abuse

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

Facts – In 2011 an Anti-Terrorism Task Force ("the TEK") was established as a branch of the Hungarian police. Its competence was defined in section 7/E of the Police Act, as amended in 2011, and in the National Security Act. In their application to the European Court, the applicants complained that the legislation violated Article 8 of the Convention because it was not sufficiently detailed and precise and did not provide sufficient guarantees against abuse and arbitrariness.

Law – Article 8: Under the legislation, two situations could entail secret surveillance by the TEK, namely, the prevention, tracking and repelling of terrorist acts in Hungary and the gathering of intelligence necessary for rescuing Hungarian citizens in distress abroad. The TEK was entitled to search and keep under surveillance homes secretly, to check post and parcels, to monitor electronic communications and computer data transmissions and to make recordings of any data acquired through these methods. The Court found that these measures constituted interference by a public authority with the exercise of the applicants' right to respect for private life, home and correspondence.

In the context of secret surveillance measures, the foreseeability requirement did not compel States to list in detail all situations that could prompt a decision to launch secret surveillance operations. However, in matters affecting fundamental rights legislation granting discretion to the executive in the sphere of national security had to indicate the scope of such discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. Under the relevant legislation authorisation for interception could be given in respect not only of named persons, but also of a "range of persons", a notion that was overly broad and could pave the way for the unlimited surveillance of a large number of citizens. The legislation did not clarify how that notion was to be applied in practice and the authorities were not required to demonstrate the actual or presumed relation between the persons or range of persons concerned and the prevention of any terrorist threat. In the Court's view, it would defy the purpose of government efforts to keep terrorism at bay, and thus restore citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically replaced by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques. In the present case, it could not be ruled out that the domestic provisions could be interpreted to enable strategic, large-scale interception. That was a matter of serious concern.

In the context of secret surveillance, the need for the interference to be "necessary in a democratic society" had to be interpreted as requiring that any measures taken should be strictly necessary both, as a general consideration, to safeguard democratic institutions and, as a particular consideration, to obtain essential intelligence in an individual operation. Any measure of secret surveillance which did not

fulfil the strict necessity criterion would be prone to abuse by the authorities. In this connection, the Court noted the absence from the legislation of safeguards such as a requirement for prior judicial authorisation of interceptions or of clear provisions governing the frequency of renewals of surveillance warrants. Although surveillance measures were subject to prior authorisation by the Minister of Justice, such supervision was eminently political and inherently incapable of ensuring the requisite assessment of strict necessity. For the Court, supervision by a politically responsible member of the executive did not provide the necessary guarantees.
The Court accepted that situations of extreme urgency could arise in which a requirement for prior judicial control would run the risk of losing precious time. It emphasised, however, that in such cases any surveillance measures authorised ex ante by a non-judicial authority had to be subject to a post factum judicial review. The Court noted that under the Hungarian system the executive was required to give account in general terms of such operations to a parliamentary committee. However, it was not persuaded that this reporting procedure, which did not appear to be public, was able to provide redress in respect of any individual grievances caused by secret surveillance or to control effectively the daily functioning of the surveillance organs. Moreover, the domestic law did not provide a judicial-control mechanism that could be triggered by those subject to secret surveillance, as the complaint procedure did not foresee any kind of subsequent notification of the surveillance measures to the citizens subjected to them. Furthermore, complaints were to be investigated by the Minister of Home Affairs, who did not appear to be sufficiently independent.

It followed from the above considerations that the legislation did not provide sufficiently precise, effective and comprehensive safeguards on the ordering, execution and potential redressing of surveillance measures.

Conclusion: violation

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

Facts: The Interception of Communications Act 1985 made it an offence intentionally to intercept communications by post or by means of a public telecommunications system. However, the Secretary of State was authorised to issue a warrant permitting the examination of communications if it was considered necessary in the interests of national security, to prevent or detect serious crime or to safeguard the State's economic well-being. Warrants could be issued in respect of communications (whether internal or external) linked to a particular address or person, or (under section 3(2) of the Act) to external communications generally, with no restriction on the person or premises concerned. Section 6 of the Act required the Secretary of State to make such arrangements as he considered necessary to ensure safeguards against abuses of power. Arrangements were reportedly put in place, but their precise details were not disclosed in the interests of national security. The Act also provided for a tribunal (the Interception of Communications Tribunal – ICT) to investigate complaints from any person who believed their communications had been intercepted and for the appointment of a Commissioner with reporting and review powers.

The applicants were a British and two Irish civil-liberties organisations. They alleged that between 1990 and 1997 their telephone, facsimile, e-mail and data communications, including legally privileged and confidential information, had been intercepted by an Electronic Test Facility operated by the British Ministry of Defence. Although they had lodged complaints with the ICT, the Director of Public Prosecutions and the Investigatory Powers Tribunal (IPT) challenging the lawfulness of the interceptions, the domestic authorities found that there had been no contravention of the 1985 Act. The IPT specifically found that the right to intercept and access material covered by a warrant, and the criteria by reference to which it was exercised, were sufficiently accessible and foreseeable to be in accordance with law.

Law: The mere existence of legislation which allowed communications to be monitored secretly entailed a surveillance threat for all those to whom it might be applied and so constituted an interference with the applicants' rights. Section 3(2) of the 1985 Act allowed the British authorities a virtually unlimited discretion to intercept any communications between the United Kingdom and an external receiver described in the warrant. Warrants covered very broad classes of communications and, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had their communication intercepted. The authorities also had wide discretion to decide which communications from those physically captured should be listened to or read.

Although during the relevant period there had been internal regulations, manuals and instructions to provide for procedures to protect against abuse of power, and although the Commissioner appointed under the 1985 Act to oversee its workings had reported each year that the "arrangements" were satisfactory, the nature of those "arrangements" had not been contained in legislation or otherwise made available to the public. Further, although the Government had expressed concern that the publication of information regarding those arrangements during the period in question might have damaged the efficiency of the intelligence-gathering system or given rise to a security risk, the Court noted that extensive extracts from the Interception of Communications Code of Practice were now in the public domain, which suggested that it was possible to make public certain details about the operation of a scheme of external surveillance without compromising national security. In conclusion, domestic law at the relevant time had not 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 State to intercept and examine external communications. In particular, it had not set out in a form accessible to the public any indication of the procedure to be followed for examining, sharing, storing and destroying intercepted material. The interference was not therefore "in accordance with the law".

Conclusion: violation

Strategic monitoring of telecommunications. Safeguards regarding media freedom

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

Facts: In 1994 the Act of 13 August 1968 on Restrictions on the Secrecy of Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses), also

called “the G 10 Act” (See Klass and Others v. Germany, judgment of 6 September 1978, Series A no. 28) 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 concern the extension of the powers of the Federal Intelligence Service (Bundesnachrichtendienst) 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. The first applicant, a German national, is a freelance journalist; the second applicant, a Uruguayan national, took telephone messages for the first applicant and passed them on to her. In 1995 the applicants lodged a constitutional complaint with the Federal Constitutional Court challenging the new amendments.

Article 8 – Restating earlier case-law, the Court notes that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants’ rights under Article 8, irrespective of any measures actually taken against them. The transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted, constitutes a further separate interference with the applicants’ rights under Article 8.

As to whether these interferences are “in accordance with the law”, the Court notes that the term “law” within the meaning of the Convention refers back to national law, including rules of public international law applicable in the State concerned; as regards allegations that a respondent State has violated international law by breaching the territorial sovereignty of a foreign State, the Court requires proof in the form of concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign State and therefore contrary to international law. The impugned provisions of the amended G 10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.

As to the statutory basis of the amended G 10 Act, the Court accepts the judgment of the Federal Constitutional court that it satisfies the Basic Law and finds no arbitrariness in its application. As to the quality of the law, firstly, its accessibility raises no problem; secondly, the Court concludes that the impugned provisions of the G 10 Act, seen in their legislative context, contained the minimum safeguards against arbitrary interference as defined in the Court’s case-law and therefore gave citizens an adequate indication as to the circumstances in which and the conditions on which the public authorities were empowered to resort to monitoring measures, and the scope and manner of exercise of the authorities’ discretion.

The “legitimate aims” pursued were to safeguard national security and/or to prevent crime.

As to whether the interferences were "necessary in a democratic society", the Court recognises that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for protecting national security. Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse. As to strategic monitoring per se, although the amended G 10 Act broadens the range of subjects in respect of which it can be carried out, safeguards against abuse were spelled out in detail and the Federal Constitutional Court in fact raised the threshold in respect of at least one crime; the Court is satisfied that there was an administrative procedure designed to ensure that measures were not ordered haphazardly, irregularly or without due and proper consideration.

As regards supervision and review of monitoring measures, the system of supervision was essentially the same as that found by the Court in its *Klass and Others* judgment not to violate the Convention; there is no reason to reach a different conclusion in the present case. As to the transmission of non-anonymous personal data obtained by the Federal Intelligence Service to the Federal Government, the Court accepts that transmission of personal – as opposed to anonymous – data might prove necessary. The additional safeguards introduced by the Federal Constitutional Court, namely that the personal data contained in the report to the Federal Government were marked and remain connected to the purposes which had justified their collection, are appropriate for the purpose of limiting the use of the information obtained to what is necessary to serve the purpose of strategic monitoring. As to the transmission of personal data to, among other authorities, the Offices for the Protection of the Constitution, the Court notes that the crimes for which this was possible were limited to certain designated serious criminal offences and that following the Federal Constitutional Court's judgment such transmission, which had to be recorded in minutes, was only possible if the suspicion that someone had committed such an offence was based on specific facts as opposed to mere factual indications; the safeguards against abuse, as thus strengthened by the Federal Constitutional Court, were adequate.

As to the destruction of personal data, an acceptable procedure for verifying whether the conditions were met was in place; moreover, the Federal Constitutional Court had ruled that data which were still needed for court proceedings could not be destroyed immediately and had extended the supervisory powers of the G 10 Commission to cover the entire process of using data up to and including their destruction.

Finally, as to the notification of persons whose communications had been monitored, this was to be done as soon as possible without jeopardising the purpose of the monitoring; rules contained in the judgment of the Federal Constitutional Court prevented the duty of notification from being circumvented, save in cases where the data were destroyed within three months without ever having been used.

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 an interference to her right, in her capacity as a journalist, to freedom of expression. The Court finds, on the reasons set out under Article 8, that this interference is prescribed by law and pursues a legitimate aim. As to necessity in a democratic society, the Court notes that strategic surveillance was not aimed at monitoring journalists; generally the authorities would know

only when examining the intercepted telecommunications, if at all, that a journalist's conversation had been monitored. Surveillance measures were, in particular, not directed at uncovering journalistic sources. The interference with freedom of expression by means of strategic monitoring cannot, therefore, be characterised as particularly serious. 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, having regard to its findings under Article 8, 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.

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, a former systems administrator with the United States National Security Agency (NSA), 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 resulting interference with their rights under Article 8 of the Convention was not "in accordance with the law". In their submission, the receipt of information from foreign intelligence agencies has no basis in domestic law and an there are no safeguards or control in relation to:

> a) the circumstances in which the UK intelligence services can request foreign intelligence agencies to intercept communications and/or to give the UK access to stored data that has been obtained by interception; and
> b) the extent to which the UK intelligence services can use, analyse, disseminate and store data solicited and/or received from foreign intelligence agencies and the process by which such data must be destroyed.

Further, in relation to the interception of communications directly by GCHQ, the applicants submit that the statutory regime applying to external communications warrants does not comply with the minimum standards outlined by the Court in its case-law.

Lastly, 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.

Communicated under Article 8 of the Convention