

## Hebrew University & University of Essex Surveillance Workshop Series

### Workshop 1 – Necessity and Proportionality

#### Brief overview of (some) relevant case law

#### Justifications for interference: the necessity/strict necessity test

- 232. As to the question whether an interference was “necessary in a democratic society” in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant’s right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the “interference” to what is “necessary in a democratic society” (see *Klass and Others*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, § 106; *Kvasnica v. Slovakia*, no. [72094/01](#), § 80, 9 June 2009; and *Kennedy*, cited above, §§ 153 and 154). [para 232, *Zakharov v. Russia*, Judgment, European Court of Human Rights, Application No. 47173/06, 4 December 2015]
- In the circumstances, the lawfulness of the interference is closely related to the question whether the “necessity” test has been complied with in respect of the “section 7/E (3) surveillance” regime and it is therefore appropriate for the Court to address jointly the “in accordance with the law” and “necessity” requirements (see *Kvasnica*, cited above, § 84). [para 58, *Szabo and Vissy v. Hungary*, Judgment, European Court of Human Rights, Application No. 37138/14, 12 January 2016]
- 72. Quite apart from what transpires from section 53(2) of the National Security Act, the Court recalls at this point that in *Klass and Others* it held that “powers of secret surveillance of citizens ... are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions” (see *Klass and Others*, cited above, § 42, quoted in paragraph 54 above). Admittedly, the expression “strictly necessary” represents at first glance a test different from the one prescribed by the wording of paragraph 2 of Article 8, that is, “necessary in a democratic society”. [para 72, *Szabo and Vissy v. Hungary*, Judgment, European Court of Human Rights, Application No. 37138/14, 12 January 2016]

- 73. However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity (see paragraphs 23 and 24 above) – an approach it considers convenient to endorse. Moreover, particularly in this context the Court notes the absence of prior judicial authorisation for interceptions, the importance of which will be examined below in paragraphs 75 *et seq.* This safeguard would serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of "persons concerned identified ... as a range of persons" by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case (see, *mutatis mutandis*, *Roman Zakharov*, cited above, § 249). It is only in this way that the need for safeguards to ensure that emergency measures are used sparingly and only in duly justified cases can be satisfied (see *Roman Zakharov*, cited above, § 266). [para 73, *Szabo and Vissy v. Hungary*, Judgment, European Court of Human Rights, Application No. 37138/14, 12 January 2016]
- "As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight." [para 51 *Digital Rights Ireland Ltd v. Minister for Communications and Others*, Judgment, Court of Justice of the European Union, Cases C-293/12 and C-594/12, 8 April 2014]
- "So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary" [para 52 *Digital Rights Ireland Ltd v. Minister for Communications and Others*, Judgment, Court of Justice of the European Union, Cases C-293/12 and C-594/12, 8 April 2014]

## Proportionality

- "...according to settled-case law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives" [para 46 *Digital Rights Ireland Ltd v. Minister for Communications and Others*, Judgment, Court of Justice of the European Union, Cases C-293/12 and C-594/12, 8 April 2014]
- "...since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data." [para 115, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Deptment v. Watson and others*, Judgment, Grand Chamber, European Court of Justice, Cases C-203/15, C-698/15, 21 December 2016]

## Rights implications

- "...it must be emphasised that the obligation imposed on providers of electronic communications services, by national legislation such as that at issue in the main proceedings, to retain traffic data in order, when necessary, to make that data available to the competent national authorities, raises questions relating to compatibility not only with Articles 7 and 8 of the Charter, which are expressly referred to in the questions referred for a preliminary ruling, but also with the freedom of expression guaranteed in Article 11 of the Charter [...]" [para 92, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Deptment v. Watson and others*, Judgment, Grand Chamber, European Court of Justice, Cases C-203/15, C-698/15, 21 December 2016]

## ‘Serious Crime’

- "It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest [...] The same is true of the fight against serious crime in order to ensure public security" [para 42, *Digital Rights Ireland Ltd v. Minister for Communications and Others*, Judgment, Court of Justice of the European Union, Cases C-293/12 and C-594/12, 8 April 2014]
- "Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure" [para 102, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Deptment v. Watson and others*, Judgment, Grand Chamber, European Court of Justice, Cases C-203/15, C-698/15, 21 December 2016]

- "...since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data." [para 115, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Deptment v. Watson and others*, Judgment, Grand Chamber, European Court of Justice, Cases C-203/15, C-698/15, 21 December 2016]

### Oversight, including authorisation

- 233. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure (see *Klass and Others*, cited above, §§ 55 and 56). [para 233, *Zakharov v. Russia*, Judgment, European Court of Human Rights, Application No. 47173/06, 4 December 2015]
- 248. It is significant that the OSAA does not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national, military, economic or ecological security. It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse (see, for similar reasoning, *Iordachi and Others*, cited above, § 46).  
249. That being said, the Court does not lose sight of the fact that prior judicial authorisation for interceptions is required in Russia. Such judicial authorisation may serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of "a person who may have information about a criminal offence", "a person who may have information relevant to the criminal case", and "events or activities endangering Russia's national, military, economic or ecological security" by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case. The Court accepts that the requirement of prior judicial authorisation constitutes an important

safeguard against arbitrariness. The effectiveness of that safeguard will be examined below. [paras 248, 249, *Zakharov v. Russia*, Judgment, European Court of Human Rights, Application No. 47173/06, 4 December 2015]

- 260. Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means (see *Klass and Others*, cited above, § 51; *Association for European Integration and Human Rights and Ekimdzhiiev*, cited above, §§ 79 and 80; *Iordachi and Others*, cited above, § 51; and *Kennedy*, cited above, §§ 31 and 32). [para 260, *Zakharov v. Russia*, Judgment, European Court of Human Rights, Application No. 47173/06, 4 December 2015] *This refers to individually targeted surveillance (of content) hence the requirement of a reasonable suspicion vis-a-vis a specific individual*
- 261. The Court notes that in Russia judicial scrutiny is limited in scope. Thus, materials containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures may not be submitted to the judge and are therefore excluded from the court's scope of review (see paragraph 37 above). The Court considers that the failure to disclose the relevant information to the courts deprives them of the power to assess whether there is a sufficient factual basis to suspect the person in respect of whom operational-search measures are requested of a criminal offence or of activities endangering national, military, economic or ecological security (see, *mutatis mutandis*, *Liu*, cited above, §§ 59-63). The Court has earlier found that there are techniques that can be employed which both accommodate legitimate security concerns about the nature and sources of intelligence information and yet accord the individual a substantial measure of procedural justice (see, *mutatis mutandis*, *Chahal v. the United Kingdom*, 15 November 1996, § 131, *Reports of Judgments and Decisions* 1996-V). [para 261, *Zakharov v. Russia*, Judgment, European Court of Human Rights, Application No. 47173/06, 4 December 2015]
- 262. Furthermore, the Court observes that in Russia the judges are not instructed, either by the CCrP or by the OSAA, to verify the existence of a "reasonable suspicion" against the person concerned or to apply the "necessity" and "proportionality" test". At the same time, the Court notes that the Constitutional Court has explained in its decisions that the burden of proof is on the requesting agency to show that interception is necessary and that the judge examining an interception request should verify the grounds for that measure and grant authorisation only if he or she is persuaded that interception is lawful, necessary and justified. The Constitutional Court has also held that the judicial decision authorising interception should contain reasons and refer to specific grounds for

suspecting that a criminal offence has been committed, or is ongoing, or is being plotted or that activities endangering national, military, economic or ecological security are being carried out, as well as that the person in respect of whom interception is requested is involved in these criminal or otherwise dangerous activities (see paragraphs 40 to 42 above). The Constitutional Court has therefore recommended, in substance, that when examining interception authorisation requests Russian courts should verify the existence of a reasonable suspicion against the person concerned and should authorise interception only if it meets the requirements of necessity and proportionality. [para 262, *Zakharov v. Russia*, Judgment, European Court of Human Rights, Application No. 47173/06, 4 December 2015]

## Safeguards

- 56. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; the definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed (see *Huwig v. France*, 24 April 1990, § 34, Series A no. 176-B; *Amann v. Switzerland* [GC], no. [27798/95](#), §§ 56-58, ECHR 2000-11; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, Reports 1998-V; *Prado Bugallo v. Spain*, no. [58496/00](#), § 30, 18 February 2003; *Weber and Saravia*, cited above, § 95; *Association for European Integration*, cited above, § 76; and *Roman Zakharov*, cited above, § 231). [para 56, *Szabo and Vissy v. Hungary*, Judgment, European Court of Human Rights, Application No. 37138/14, 12 January 2016]
- 57. When balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society" (see *Klass and Others*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, §106; *Kvasnica v. Slovakia*, no. [72094/01](#), § 80, 9 June 2009; *Kennedy*, cited above, §§ 153 and 154; and *Roman Zakharov*, cited above, § 232). [para

57, *Szabo and Vissy v. Hungary*, Judgment, European Court of Human Rights, Application No. 37138/14, 12 January 2016]

- "...as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detention and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected." [para 110, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v. Watson and others*, Judgment, Grand Chamber, European Court of Justice, Cases C-203/15, C-698/15, 21 December 2016]

#### **Safeguards regarding communications data may need to be clarified**

- 70. The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile (see the CDT's submissions on this in paragraph 49 above) of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union and the European Parliament (see paragraphs 23 and 25 above). This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices. However, it is not warranted to embark on this matter in the present case, since the Hungarian system of safeguards appears to fall short even of the previously existing principles. [para 70, *Szabo and Vissy v. Hungary*, Judgment, European Court of Human Rights, Application No. 37138/14, 12 January 2016]