# *Computerrecht* 2016/86

Europees Hof voor de Rechten van de Mens 4 december 2015, nr. 47143/06
(Dean Spielmann, *President*, Josep Casadevall, Guido Raimondi, Ineta Ziemele, Mark Villiger, Luis López Guerra, Khanlar Hajiyev, Angelika Nußberger, Julia Laffranque, Linos-Alexandre Sicilianos, Erik Møse, André Potocki, Paul Lemmens, Helena Jäderblom, Faris Vehabović, Ksenija Turković, Dmitry Dedov, judges, and Lawrence Early, *Jurisconsult*)
m.nt. S.J. Eskens[1]

Art. 8 EVRM

NJB 2016/402
ECLI:CE:ECHR:2015:1204JUD004714306

**In Roman Zakharov/Rusland bevestigt het Europees Hof voor de Rechten van de Mens de strenge vereisten waar het juridisch kader voor heimelijk onderscheppen van telefoon- en internetverkeer aan moet voldoen onder het Europees Verdrag voor de Rechten van de Mens ("EVRM"). Het Hof concludeert dat Russische aftapwetgeving in strijd is met het recht op privacy, zoals beschermd door artikel 8 EVRM. In een zaak die kort daarop volgt, concludeert het Hof dat Hongaarse wetgeving voor massale surveillance een schending met het EVRM oplevert. De vraag is nu of het in bulk onderscheppen van elektronische communicatie per definitie strijdig is met het EVRM.**

Arrest in de zaak van Roman Zakharov/Rusland

**THE FACTS**

I. ***THE CIRCUMSTANCES OF THE CASE***

7. The applicant was born in 1977 and lives in St Petersburg.

8. The applicant is the editor-in-chief of a publishing company and of an aviation magazine. He is also the chairperson of the St Petersburg branch of the Glasnost Defence Foundation, an NGO monitoring the state of media freedom in the Russian regions, which promotes the independence of the regional mass media, freedom of speech and respect for journalist's rights, and provides legal support, including through litigation, to journalists.

9. He was subscribed to the services of several mobile network operators.

10. On 23 December 2003 he brought judicial proceeding against three mobile network operators, claiming that there had been an interference with his right to the privacy of his telephone communications. He claimed that pursuant to Order no. 70 (see paragraphs 115 to 122 below) of the Ministry of Communication's predecessor, the State Committee for Communications and Information Technologies, the mobile network operators had installed equipment which permitted the Federal Security Service ("the FSB") to intercept all telephone communications without prior judicial authorisation. The applicant argued that Order no. 70, which had never been published, unduly restricted his right to privacy. He asked the court to issue an injunction ordering the removal of the equipment installed pursuant to Order no. 70, and to ensure that access to mobile telephone communications was given to authorised persons only. The Ministry of Communications and Information Technologies (hereafter "the Ministry of Communications") and the St Petersburg and Leningrad Region Department of the FSB were joined as a third party to the proceedings.

11. On 5 December 2005 the Vasileostrovskiy District Court of St Petersburg dismissed the applicant's claims.

[…]

13. On 26 April 2006 the St Petersburg City Court upheld the judgment on appeal.

[…]

II. ***RELEVANT DOMESTIC LAW***

*C. General provisions on interception of communications*

25. The interception of communications is governed by the Operational-Search Activities Act of 12 August 1995 (no. 144-FZ, hereafter "the OSAA"), applicable to the interception of communications both in the framework of criminal proceedings and outside such framework; and the Code of Criminal Procedure of 18 December 2001 (no. 174-FZ, in force since 1 July 2002, hereafter "the CCrP"), applicable only to the interception of communications in the framework of criminal proceedings.

26. The aims of operational-search activities are: (1) the detection, prevention, suppression and investigation of criminal offences and the identification of persons conspiring to commit, committing, or having committed a criminal offence; (2) the tracing of fugitives from justice and missing persons; (3) obtaining information about events or activities endangering the national, military, economic or ecological security of the Russian Federation (section 2 of the OSAA). On 25 December 2008 that section was amended and a further aim, that of obtaining information about property subject to confiscation, was added.

27. State officials and agencies performing operational-search activities must show respect for the private and family life, home and correspondence of citizens. It is prohibited to perform operational-search activities to achieve aims or objectives other than those specified in the Act (section 5(1) and (2) of the OSAA).

[…]

29. Operational-search activities include, *inter alia*, the interception of postal, telegraphic, telephone and other forms of communication and the collection of data from technical channels of communication. The Act stipulates that audio and video recording, photography, filming and other technical means may be used during operational-

1 Sarah Johanna Eskens, promovenda aan het Instituut voor Informatierecht (IViR), Universiteit van Amsterdam.

search activities, provided that they are not harmful to the life or health of those involved or to the environment. Operational-search activities involving the interception of postal, telegraphic, telephone and other forms of communication and collection of data from technical channels of communication using equipment installed by communications service providers is carried out by technical means by the FSB and the agencies of the Ministry of the Interior, in accordance with decisions and agreements signed between the agencies involved (section 6 of the OSAA).
[…]

*D. Situations that may give rise to interception of communications*

31. Operational-search activities involving interference with the constitutional right to the privacy of postal, telegraphic and other communications transmitted by means of a telecommunications network or mail services, or within the privacy of the home, may be conducted following the receipt of information (1) that a criminal offence has been committed or is ongoing, or is being plotted; (2) about persons conspiring to commit, or committing, or having committed a criminal offence; or (3) about events or activities endangering the national, military, economic or ecological security of the Russian Federation (section 8(2) of the OSAA).

32. The OSAA provides that interception of telephone and other communications may be authorised only in cases where a person is suspected of, or charged with, a criminal offence of medium severity, a serious offence or an especially serious criminal offence, or may have information about such an offence (section 8(4) of the OSAA). The CCrP also provides that interception of telephone and other communications of a suspect, an accused or other person may be authorised if there are reasons to believe that they may contain information relevant for the criminal case in respect of a criminal offence of medium severity, a serious offence or an especially serious criminal offence (Article 186 § 1 of the CCrP).

33. Article 15 of the Criminal Code provides that "offences of medium severity" are premeditated offences for which the Criminal Code prescribes a maximum penalty of between three and five years' imprisonment and unpremeditated offences for which the Criminal Code prescribes a maximum penalty of more than three years' imprisonment. "Serious offences" are premeditated offences for which the Criminal Code prescribes a maximum penalty of between five and ten years' imprisonment. "Especially serious offences" are premeditated offences for which the Code prescribes a maximum penalty of more than ten years' imprisonment or a harsher penalty.
[…]

*J. Obligations of communications service providers*
[…]

*3. Technical requirements for equipment to be installed by communications service providers*

114. The main characteristics of the system of technical facilities enabling operational-search activities to be carried out ("Система технических средств для обеспечения функций оперативно-разыскных мероприятий" ('COPM'), hereafter referred to as "the SORM") are outlined in a number of orders and regulations issued by the Ministry of Communications.

*(a) Order no. 70*

115. Order no. 70 on the technical requirements for the system of technical facilities enabling the conduct of operational-search activities using telecommunications networks, issued by the Ministry of Communications on 20 April 1999, stipulates that equipment installed by communications service providers must meet certain technical requirements, which are described in the addendums to the Order. The Order, with the addendums, has been published in the Ministry of Communications' official magazine *SvyazInform*, distributed through subscription. It can also be accessed through a privately-maintained internet legal database, which reproduced it from the publication in *SvyazInform*.

116. Addendums nos. 1 and 3 describe the technical requirements for the SORM on mobile telephone networks. They specify that interception of communications is performed by law-enforcement agencies from a remote-control terminal connected to the interception equipment installed by the mobile network operators. The equipment must be capable, *inter alia*, of (a) creating databases of interception subjects, to be managed from the remote-control terminal; (b) intercepting communications and transmitting the data thereby obtained to the remote-control terminal; (c) protecting the data from unauthorised access, including by the employees of the mobile network operator; (d) providing access to subscriber address databases (paragraphs 1.1. and 1.6 of Addendum no. 1).
[…]

**THE LAW**

I. ***ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION***

148. The applicant complained that the system of covert interception of mobile telephone communications in Russia did not comply with the requirements of Article 8 of the Convention, which reads as follows:

> "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 is 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 pre-

vention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

*A. Admissibility*

149. The Government submitted that the applicant could not claim to be a victim of the alleged violation of his right to respect for his private life or correspondence (see paragraphs 152 to 157 below). Moreover, he had not exhausted domestic remedies (see paragraphs 219 to 226 below).

150. The Court considers that the Government's objections are so closely linked to the substance of the applicant's complaint that they must be joined to the merits.

151. The Court further notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It is not inadmissible on any other grounds. It must therefore be declared admissible.

*B. Merits*

*1. The applicant's victim status and the existence of an "interference"*

[…]

*(b) The Court's assessment*

163. The Court observes that the applicant in the present case claims that there has been an interference with his rights as a result of the mere existence of legislation permitting covert interception of mobile telephone communications and a risk of being subjected to interception measures, rather than as a result of any specific interception measures applied to him.

*(i) Summary of the Court's case-law*

[…]

*(ii) Harmonisation of the approach to be taken*

170. The Court considers, against this background, that it is necessary to clarify the conditions under which an applicant can claim to be the victim of a violation of Article 8 without having to prove that secret surveillance measures had in fact been applied to him, so that a uniform and foreseeable approach may be adopted.

171. In the Court's view the *Kennedy* approach is best tailored to the need to ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and of the Court. Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. As the Court underlined in *Kennedy*, where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified (see *Kennedy*, cited above, § 124). In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto*, is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.

172. The *Kennedy* approach therefore provides the Court with the requisite degree of flexibility to deal with a variety of situations which might arise in the context of secret surveillance, taking into account the particularities of the legal systems in the member States, namely the available remedies, as well as the different personal situations of applicants.

*(iii) Application to the present case*

173. It is not disputed that mobile telephone communications are covered by the notions of "private life" and "correspondence" in Article 8 § 1 (see, for example, *Liberty and Others*, cited above, § 56).

[…]

175. The Court notes that the contested legislation institutes a system of secret surveillance under which any person using mobile telephone services of Russian providers can have his or her mobile telephone communications intercepted, without ever being notified of the surveillance. To that extent, the legislation in question directly affects all users of these mobile telephone services.

176. Furthermore, for the reasons set out below (see paragraphs 286 to 300), Russian law does not provide for effective remedies for a person who suspects that he or she was subjected to secret surveillance.

177. In view of the above finding, the applicant does not need to demonstrate that, due to his personal situation, he is at risk of being subjected to secret surveillance.

178. Having regard to the secret nature of the surveillance measures provided for by the contested legislation, the broad scope of their application, affecting all users of mobile telephone communications, and the lack of effective means to challenge the alleged application of secret surveillance measures at domestic level, the Court considers an examination of the relevant legislation *in abstracto* to be justified.

179. The Court therefore finds that the applicant is entitled to claim to be the victim of a violation of the Convention, even though he is unable to allege that he has been subject to a concrete measure of surveillance in support of his application. For the same reasons, the mere existence of the contested legislation amounts in itself to an interference with the exercise of his rights under Article 8. The Court therefore dismisses the Government's objection concerning the applicant's lack of victim status.

*2. The justification for the interference*

[…]

*(b) The Court's assessment*

*(i) General principles*

[…]

228. The Court notes from its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects (see, among many other authorities, *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000-V;*S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 95, ECHR 2008; and *Kennedy*, cited above, § 151).

229. The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see Malone, cited above, § 67; *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116; *Huvig v. France*, 24 April 1990, § 29, Series A no. 176-B; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, *Reports of Judgments and Decisions* 1998-V; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 75).

230. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, § 68; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; and *Weber and Saravia*, cited above, § 94).

231. 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; a 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 *Huvig*, cited above, § 34; *Amann v. Switzerland* [GC], no. 27798/95, §§ 56-58, ECHR 2000-II; *Valenzuela Contreras*, cited above, § 46; *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 76).

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 it's 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).

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).

234. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Klass and Others*, cited above, § 57, and *Weber and Saravia*, cited above, § 135) or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications (see *Kennedy*, cited above, § 167).

*(ii) Application of the general principles to the present case*

[…]

*(β) Scope of application of secret surveillance measures*

[…]

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.

[…]

*(ε) Authorisation of interceptions*

*Authorisation procedures*

[…]

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 Ekimdzhiev*, cited above, §§ 79 and 80; *Iordachi and Others*, cited above, § 51; and *Kennedy*, cited above, §§ 31 and 32).

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*, *Cha-*

*hal v. the United Kingdom*, 15 November 1996, § 131, *Reports of Judgments and Decisions* 1996-V).

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.

263. However, the Court observes that the domestic law does not explicitly require the courts of general jurisdiction to follow the Constitutional Court's opinion as to how a legislative provision should be interpreted if such opinion has been expressed in a decision rather than a judgment (see paragraph 106 above). Indeed, the materials submitted by the applicant show that the domestic courts do not always follow the above-mentioned recommendations of the Constitutional Court, all of which were contained in decisions rather than in judgments. Thus, it transpires from the analytical notes issued by District Courts that interception requests are often not accompanied by any supporting materials, that the judges of these District Courts never request the interception agency to submit such materials and that a mere reference to the existence of information about a criminal offence or activities endangering national, military, economic or ecological security is considered to be sufficient for the authorisation to be granted. An interception request is rejected only if it is not signed by a competent person, contains no reference to the offence in connection with which interception is to be ordered, or concerns a criminal offence in respect of which interception is not permitted under domestic law (see paragraph 193 above). Thus, the analytical notes issued by District Courts, taken together with the statistical information for the period from 2009 to 2013 provided by the applicant (see paragraph 194 above), indicate that in their everyday practice Russian courts do not verify whether there is a "reasonable suspicion" against the person concerned and do not apply the "necessity" and "proportionality" test.

264. Lastly, as regards the content of the interception authorisation, it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information (see *Klass and Others*, cited above, § 51; *Liberty and Others*, cited above, §§ 64 and 65; *Dumitru Popescu* (no. 2), cited above, § 78; *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 80; and *Kennedy*, cited above, § 160).

265. The Court observes that the CCrP requires that a request for interception authorisation must clearly mention a specific person whose communications are to be intercepted, as well as the duration of the interception measure (see paragraph 46 above). By contrast, the OSAA does not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation. As a result, courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed. Some authorisations do not mention the duration for which interception is authorised (see paragraph 193 above). The Court considers that such authorisations, which are not clearly prohibited by the OSAA, grant a very wide discretion to the law-enforcement authorities as to which communications to intercept, and for how long.

[…]

267. In view of the above considerations the Court considers that the authorisation procedures provided for by Russian law are not capable of ensuring that secret surveillance measures are not ordered haphazardly, irregularly or without due and proper consideration.

[…]

*(ζ) Supervision of the implementation of secret surveillance measures*

272. The Court notes at the outset that Order no. 70 requires that the equipment installed by the communications service providers does not record or log information about interceptions (see paragraph 120 above). The Court has found that an obligation on the intercepting agencies to keep records of interceptions is particularly important to ensure that the supervisory body had effective access to details of surveillance activities undertaken (see *Kennedy*, cited above, § 165). The prohibition on logging or recording interceptions set out in Russian law makes it impossible for the supervising authority to discover interceptions carried out without proper judicial authorisation. Combined with the law-enforcement authorities' technical ability, pursuant to the same Order no. 70, to intercept directly all communications, this provision renders any supervision arrangements incapable of detecting unlawful interceptions and therefore ineffective.

[…]

279. In contrast to the supervisory bodies cited above, in Russia prosecutors are appointed and dismissed by the Prosecutor General after consultation with the regional executive authorities (see paragraph 70 above). This fact may raise doubts as to their independence from the executive.

280. Furthermore, it is essential that any role prosecutors have in the general protection of human rights does not give rise to any conflict of interest (see *Menchinskaya v. Russia*, no. 42454/02, §§ 19 and 38, 15 January 2009). The Court observes that prosecutors' offices do not specialise in supervision of interceptions (see paragraph 71 above). Such supervision is only one part of their broad and diversified functions, which include prosecution and supervision of criminal investigations. In the framework of their prosecuting functions, prosecutors give their approval to all interception requests lodged by investigators in the framework of criminal proceedings (see paragraph 44 above). This blending of functions within one prosecutors' office, with the same office giving approval to requests for interceptions and then supervising their implementation, may also raise doubts as to the prosecutors' independence (see, by way of contrast, *Ananyev and Others v. Russia*, nos. 42525/07 and 60800/08, § 215, 10 January 2012, concerning supervision by prosecutors of detention facilities, where it was found that prosecutors complied with the requirement of independence *vis-à-vis* the penitentiary system's bodies).

281. Turning now to the prosecutors' powers and competences, the Court notes that it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required (see *Kennedy*, cited above, § 166). Russian law stipulates that prosecutors are entitled to study relevant documents, including confidential ones. It is however important to note that information about the security services' undercover agents, and about the tactics, methods and means used by them, is outside the scope of prosecutors' supervision (see paragraph 74 above). The scope of their supervision is therefore limited. Moreover, interceptions performed by the FSB in the sphere of counterintelligence may be inspected only following an individual complaint (see paragraph 76 above). As individuals are not notified of interceptions (see paragraph 81 above and paragraph 289 below), it is unlikely that such a complaint will ever be lodged. As a result, surveillance measures related to counter-intelligence de facto escape supervision by prosecutors.

282. The supervisory body's powers with respect to any breaches detected are also an important element for the assessment of the effectiveness of its supervision (see, for example, *Klass and Others*, cited above, § 53, where the intercepting agency was required to terminate the interception immediately if the G10 Commission found it illegal or unnecessary; and *Kennedy*, cited above, § 168, where any intercept material was to be destroyed as soon as the Interception of Communications Commissioner discovered that the interception was unlawful). The Court is satisfied that prosecutors have certain powers with respect to the breaches detected by them. Thus, they may take measures to stop or remedy the detected breaches of law and to bring those responsible to liability (see paragraph 79 above). However, there is no specific provision requiring destruction of the unlawfully obtained intercept material (see *Kennedy*, cited above, § 168).

[…]

284. Lastly, the Court notes that it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples (see, mutatis mutandis, *Ananyev and Others*, cited above, §§ 109 and 110). However, the Russian Government did not submit any inspection reports or decisions by prosecutors ordering the taking of measures to stop or remedy a detected breach of law. It follows that the Government did not demonstrate that prosecutors' supervision of secret surveillance measures is effective in practice. The Court also takes note in this connection of the documents submitted by the applicant illustrating prosecutors' inability to obtain access to classified materials relating to interceptions (see paragraph 14 above). That example also raises doubts as to the effectiveness of supervision by prosecutors in practice.

285. In view of the defects identified above, and taking into account the particular importance of supervision in a system where law-enforcement authorities have direct access to all communications, the Court considers that the prosecutors' supervision of interceptions as it is currently organised is not capable of providing adequate and effective guarantees against abuse.

*(η) Notification of interception of communications and available remedies*

[…]

291. The Court will bear the above factors – the absence of notification and the lack of an effective possibility to request and obtain information about interceptions from the authorities – in mind when assessing the effectiveness of remedies available under Russian law.

292. Russian law provides that a person claiming that his or her rights have been or are being violated by a State official performing operational-search activities may complain to the official's superior, a prosecutor or a court (see paragraph 83 above). The Court reiterates that a hierarchical appeal to a direct supervisor of the authority whose actions are being challenged does not meet the requisite standards of independence needed to constitute sufficient protection against the abuse of authority (see, for similar reasoning, *Khan v. the United Kingdom*, no. 35394/97, §§ 45-47, ECHR 2000-V; *Dumitru Popescu (no. 2)*, cited above, § 72; and *Avanesyan*, cited above, § 32). A prosecutor also lacks independence and has a limited scope of review, as demonstrated above (see paragraphs 277 to 285 above). It remains to be ascertained whether a complaint to a court may be regarded as an effective remedy.

293. There are four judicial procedures which, according to the Government, may be used by a person wishing to complain about interception of his communications: an appeal, a cassation appeal or a supervisory-review complaint against the judicial decision authorising interception

of communications; a judicial review complaint under Article 125 of the CCrP; a judicial review complaint under the Judicial Review Act and Chapter 25 of the Code of Civil Procedure; and a civil tort claim under Article 1069 of the Civil Code. The Court will examine them in turn.

294. The first of the procedures invoked by the Government is an appeal, cassation appeal or supervisory-review complaint against the judicial decision authorising interception of communications. However, the Constitutional Court stated clearly that the interception subject had no right to appeal against the judicial decision authorising interception of his communications (see paragraph 40 above; see also *Avanesyan*, cited above, § 30). Domestic law is silent on the possibility of lodging a cassation appeal. Given that the Government did not submit any examples of domestic practice on examination of cassation appeals, the Court has strong doubts as to the existence of a right to lodge a cassation appeal against a judicial decision authorising interception of communications. At the same time, the interception subject is clearly entitled to lodge a supervisory review complaint (see paragraph 43 above). However, in order to lodge a supervisory review complaint against the judicial decision authorising interception of communications, the person concerned must be aware that such a decision exists. Although the Constitutional Court has held that it is not necessary to attach a copy of the contested judicial decision to the supervisory review complaint (ibid.), it is difficult to imagine how a person can lodge such a complaint without having at least the minimum information about the decision he or she is challenging, such as its date and the court which has issued it. In the absence of notification of surveillance measures under Russian law, an individual would hardly ever be able to obtain that information unless it were to be disclosed in the context of criminal proceedings against him or her or there was some indiscretion which resulted in disclosure.

[…]

296. As regards the judicial review complaint under the Judicial Review Act, Chapter 25 of the Code of Civil Procedure and the new Code of Administrative Procedure and a civil tort claim under Article 1069 of the Civil Code, the burden of proof is on the claimant to show that the interception has taken place and that his or her rights were thereby breached (see paragraphs 85, 95, 96 and 105 above). In the absence of notification or some form of access to official documents relating to the interceptions such a burden of proof is virtually impossible to satisfy. Indeed, the applicant's judicial complaint was rejected by the domestic courts on the ground that he had failed to prove that his telephone communications had been intercepted (see paragraphs 11 and 13 above). The Court notes that the Government submitted several judicial decisions taken under Chapter 25 of the Code of Civil Procedure or Article 1069 of the Civil Code (see paragraphs 220 to 223 above). However, all of those decisions, with one exception, concern searches or seizures of documents or objects, that is, operational-search measures carried out with the knowledge of the person concerned. Only one judicial decision concerns interception of communications. In that case the intercept subject was able to discharge the burden of proof because she had learned about the interception of her communications in the course of criminal proceedings against her.

297. Further, the Court takes note of the Government's argument that Russian law provides for criminal remedies for abuse of power, unauthorised collection or dissemination of information about a person's private and family life and breach of citizens' right to privacy of communications. For the reasons set out in the preceding paragraphs these remedies are also available only to persons who are capable of submitting to the prosecuting authorities at least some factual information about the interception of their communications (see paragraph 24 above).

298. The Court concludes from the above that the remedies referred to by the Government are available only to persons who are in possession of information about the interception of their communications. Their effectiveness is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. Accordingly, the Court finds that Russian law does not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject. […]

299. Lastly, with respect to the remedies to challenge the alleged insufficiency of safeguards against abuse in Russian law before the Russian courts, the Court is not convinced by the Government's argument that such remedies are effective (see paragraphs 156 and 225 above). As regards the possibility to challenge the OSAA before the Constitutional Court, the Court observes that the Constitutional Court has examined the constitutionality of the OSAA on many occasions and found that it was compatible with the Constitution (see paragraphs 40 to 43, 50, 82 and 85 to 87 above). In such circumstances the Court finds it unlikely that a complaint by the applicant to the Constitutional Court, raising the same issues that have already been examined by it, would have any prospects of success. Nor is the Court convinced that a challenge of Order no. 70 before the Supreme Court or the lower courts would constitute an effective remedy. Indeed, the applicant did challenge Order no. 70 in the domestic proceedings. However, both the District and City Courts found that the applicant had no standing to challenge the Order because the equipment installed pursuant to that order did not in itself interfere with the privacy of his communications (see paragraphs 10, 11 and 13 above). It is also significant that the Supreme Court found that Order no. 70 was technical rather than legal in nature (see paragraph 128 above).

300. In view of the above considerations, the Court finds that Russian law does not provide for effective remedies to a person who suspects that he or she has been subjected to secret surveillance. By depriving the subject of interception of the effective possibility of challenging interceptions retrospectively, Russian law thus eschews an important safeguard against the improper use of secret surveillance measures.

301. For the above reasons, the Court also rejects the Government's objection as to non-exhaustion of domestic remedies.

*(θ) Conclusion*

302. The Court concludes that Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications. In particular, the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity. Provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference. The domestic law permits automatic storage of clearly irrelevant data and is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial. The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when "necessary in a democratic society". The supervision of interceptions, as it is currently organised, does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice. The effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions.

303. It is significant that the shortcomings in the legal framework as identified above appear to have an impact on the actual operation of the system of secret surveillance which exists in Russia. The Court is not convinced by the Government's assertion that all interceptions in Russia are performed lawfully on the basis of a proper judicial authorisation. The examples submitted by the applicant in the domestic proceedings (see paragraph 12 above) and in the proceedings before the Court (see paragraph 197 above) indicate the existence of arbitrary and abusive surveillance practices, which appear to be due to the inadequate safeguards provided by law (see, for similar reasoning, *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 92; and, by contrast,*Klass and Others*, cited above, § 59, and *Kennedy*, cited above, §§ 168 and 169).

304. In view of the shortcomings identified above, the Court finds that Russian law does not meet the "quality of law" requirement and is incapable of keeping the "interference" to what is "necessary in a democratic society".

305. There has accordingly been a violation of Article 8 of the Convention.

[…]

**FOR THESE REASONS, THE COURT**

1. *Joins*, unanimously, to the merits the Government's objections regarding the applicant's lack of victim status and non-exhaustion of domestic remedies and *declares* the application admissible;
2. *Holds*, unanimously, that there has been a violation of Article 8 of the Convention and *dismisses* the Government's above-mentioned objections;
3. *Holds*, unanimously, that there is no need to examine the complaint under Article 13 of the Convention;
4. *Holds*, by sixteen votes to one, that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant;
5. *Holds*, unanimously,
   (a) that the respondent State is to pay the applicant, within three months, EUR 40,000 (forty thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;
6. *Dismisses*, unanimously, the remainder of the applicant's claim for just satisfaction.

Done in English and French, and delivered at a public hearing in the Human Rights Building, Strasbourg, on 4 December 2015.

Lawrence Early
Jurisconsult
Dean Spielmann
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) Concurring opinion of Judge Dedov;
(b) Partly dissenting opinion of Judge Ziemele.

D.S.
T.L.E.

**Noot**

1. ***Twee uitspraken over geheime surveillance***

In *Roman Zakharov/Rusland* bevestigt de Grote Kamer van het Europees Hof voor de Rechten van de Mens de strenge vereisten waar het juridisch kader voor geheime surveillance aan moet voldoen onder het Europees Verdrag voor de Rechten van de Mens ("EVRM"). De uitspraak is belangrijk met het oog op Nederlandse wetgeving die wordt voorbereid, zoals de nieuwe Wet op de inlichtingen- en veiligheidsdiensten en de Wet computercriminaliteit III. Maar, de uitspraak beantwoordt niet de grote vraag in het Europese debat over het aftappen van telefoon- en internetverkeer. Is het in bulk onderscheppen per definitie in strijd met het EVRM? Deze noot licht het belang van *Roman Zakharov* toe en laat zien dat de laatste vraag nog openligt, zelfs nadat

het Hof in een andere recente zaak concludeerde dat Hongaarse wetgeving voor massale surveillance mensenrechten schond.

### 2. *Een klacht over Russische aftapwetgeving*

De aanleiding voor *Roman Zakharov* is de aftap-apparatuur die Russische mobiele netwerkproviders op bevel van de regering op hun netwerken hebben geïnstalleerd. Volgens meneer Roman Zakharov kan de Russische veiligheidsdienst met deze apparatuur direct mobiel telefoonverkeer aftappen, zonder de rechterlijke machtiging die de Russische wetgeving eigenlijk vereist. De zaak betreft niet het in bulk aftappen van elektronische communicatie ("ongerichte interceptie" in Nederlands jargon), maar wetgeving op basis waarvan de Russische veiligheidsdienst aangewezen personen kan aftappen ("gerichte interceptie") – hoewel de dienst technisch gezien *al* het mobiele telefoonverkeer wel *zou kunnen* aftappen.[2] Nadat Roman Zakharov's klachten in een nationale procedure zijn afgewezen, klaagt hij bij het Hof in Straatsburg dat het enkele bestaan van de Russische aftapwetgeving een inmenging is met zijn recht op privacy, zoals beschermd door artikel 8 EVRM.[3]

Om te beginnen verheldert het Hof in *Roman Zakharov* de voorwaarden waaronder iemand in Straatsburg over aftapwetgeving kan klagen. Normaal gesproken toetst het Hof nationale wetgeving niet *in abstracto*, maar beoordeelt het alleen de toepassing van regels in een concreet geval. In het geval van geheime surveillance maakt het Hof sinds *Klass en Anderen/Duitsland* soms een uitzondering.[4] In die zaak erkende het Hof dat een verzoeker meestal niet weet dat zij "slachtoffer" is – het ontvankelijkheidsvereiste van artikel 34 EVRM – van geheime surveillance, juist omdat de surveillance in het geheim plaatsvindt. Het Hof toonde zich in *Klass en Anderen* bereid in dat soort gevallen onder omstandigheden toch slachtoffer-status toe te kennen, zodat burgers niet van rechtsbescherming worden uitgesloten. Na *Klass en Anderen* ontwikkelde het Hof verschillende methodes om te bepalen of iemand in het geval van geheime surveillance daadwerkelijk recht van klagen heeft. Met de uitspraak in *Roman Zakharov* brengt het Hof hier één lijn in aan.

De vraag of iemand bij het Hof kan klagen over aftapwetgeving, hangt voortaan af van het bereik van de regels, en van de kwaliteit van de rechtsbescherming op nationaal niveau. Ten eerste bekijkt het Hof of de verzoeker misschien is afgetapt, ofwel omdat ze behoort tot een specifieke groep personen waar de beklaagde regels op zien (bijvoorbeeld mensen die verdacht worden van terroristische plannen), *of* omdat de regels simpelweg alle gebruikers van elektronische communicatiediensten treffen, door een systeem in te stellen waaronder ieders communicatie onderschept kan worden. Ten tweede onderzoekt het Hof of het nationale rechtssysteem effectieve rechtsmiddelen biedt aan iemand die vermoedt dat ze is afgetapt. Als er geen rechtsmiddelen zijn, heeft de verzoeker sowieso recht van klagen in Straatsburg, want in zo'n geval is het niet onredelijk dat burgers het gevoel hebben dat aftapbevoegdheden worden misbruikt. Als er wel rechtsmiddelen zijn, moet de verzoeker bewijzen dat ze vanwege haar persoonlijke situatie mogelijk het risico loopt om afgetapt te worden.[5]

*In casu* stelt het Hof vast dat de beklaagde Russische wetgeving direct alle gebruikers van mobiele telefonie treft (de eerste voorwaarde), en dat het Russische recht niet voorziet in effectieve rechtsmiddelen voor iemand die vermoedt dat ze is afgetapt (de tweede voorwaarde; zie hieronder). Roman Zakharov kan dus stellen dat hij slachtoffer is in de zin van artikel 34 EVRM, en het Hof gaat door om zijn klacht inhoudelijk te onderzoeken.[6]

### 3. *Vereisten aan aftapwetgeving*

Vervolgens is het de vraag of het Russische wettelijk kader voor aftappen voldoet aan de vereisten die voortvloeien uit artikel 8 EVRM. Sinds *Klass en Anderen* heeft het Hof een aantal algemene principes ontwikkeld waar zo'n kader aan moet voldoen, en in *Roman Zakharov* zet het Hof deze principes nog eens op een rij. Wanneer het Hof wetgeving (en niet de toepassing ervan in een concreet geval) beoordeelt, legt het de nadruk op het legaliteitsvereiste van artikel 8, paragraaf 2, EVRM, en vervat hierin het noodzakelijkheidsvereiste. Ten eerste moeten de aftapregels voor de burger toegankelijk zijn, en de gevolgen ervan te voorzien.[7] "Te voorzien" betekent dat de wetgeving voldoende duidelijk moet zijn, zodat burgers inzicht hebben in de omstandigheden en voorwaarden waaronder de bevoegde instanties bevoegd zijn tot geheime interceptie van telefoon- of internetverkeer.[8]

Om machtsmisbruik bij de overheid te voorkomen, moet een aftapwet verder een minimaal aantal waarborgen omschrijven: (1) de soort misdrijven die aanleiding kunnen geven tot aftappen; (2) de categorieën personen die afgetapt kunnen worden; (3) een beperking aan de tijdsduur van aftappen; (4) een procedure voor inzage, verwerking en opslag van de verzamelde gegevens; (5) voorschriften met betrekking tot

2 Zie daarover ook Sarah St.Vincent, 'Did the European Court of Human Rights just Outlaw "Massive Monitoring of Communications" in Europe?', *Center for Democracy & Technology*, 13 januari 2016, https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/ (laatst geraadpleegd 7 mei 2016).

3 Par. 163 *Roman Zakharov*.

4 EHRM 6 september 1978, 5029/71 (*Klass en Anderen/Duitsland*).

5 Par. 171 *Roman Zakharov*. In *Roman Zakharov* spreekt het Hof van "potentially at risk of being subject to such measures", terwijl het – of de Europese Commissie voor de Rechten van de Mens – tot dan toe altijd sprak van "a reasonable likelihood" dat iemand was afgetapt; zie bijv. de ontvankelijkheidsbeslissing in ECRM 6 juli 1988, 12015/86 (*Hilton/Verenigd Koninkrijk*). De nieuwe toets lijkt lichter, en meer in het voordeel van de positie van de burger; zie hierover ook Lorna Woods, 'ECtHR case report and comment – Roman Zakharov v Russia (Grand Chamber)', *Information Law & Policy Centre at IALS*, 15 december 2015, https://infolawcentre.blogs.sas.ac.uk/2015/12/15/lorna-woods-ecthr-case-report-and-comment-roman-zakharov-v-russia-grand-chamber/ (laatst geraadpleegd 7 mei 2016).

6 Par. 173-179 *Roman Zakharov*.

7 Par. 228 *Roman Zakharov*.

8 Par. 229 *Roman Zakharov*.

het doorgeven van gegevens aan andere instanties; en (6) de omstandigheden waaronder de verzamelde gegevens vernietigd worden.[9]

Tenslotte moet de wet zodanig toezicht instellen, dat het aftappen beperkt blijft tot hetgeen noodzakelijk is in een democratische samenleving.[10] Hierbij maakt het Hof onderscheid tussen toezicht vooraf (wanneer er toestemming tot tappen wordt gegeven), toezicht terwijl het aftappen wordt uitgevoerd, en toezicht achteraf (in de vorm van toegang tot de rechter of andere rechtsmiddelen voor de burger). Op alle drie de momenten moet er toezicht zijn. Net zoals in eerdere zaken, spreekt het Hof duidelijk haar voorkeur uit voor voorafgaand rechterlijk toezicht,[11] en benadrukt het Hof dat de effectiviteit van toezicht achteraf nauw samenhangt met de vraag of het aftappen na afloop kenbaar wordt gemaakt aan de betrokkenen.[12]

### 4. *Voldoet de praktijk aan het EVRM en is er effectief toezicht?*

De toegevoegde waarde van de uitspraak in *Roman Zakharov* is dat de Grote Kamer van het Hof uitspraken van de gewone Kamer bevestigt, en zeer kritisch toepast.[13] Het Hof controleert nog uitvoeriger dan voorheen of het Russische systeem *in de praktijk* aan de vereisten van artikel 8 EVRM voldoet, en of het toezicht onafhankelijk en *effectief* is. Hierbij is het aan de overheid om de effectiviteit van het toezicht met voorbeelden te demonstreren.[14] Het Hof noteert bijvoorbeeld dat er in Rusland in theorie voorafgaand rechterlijk toezicht is op aftappen.[15] Maar, zo constateert het Hof, Russische rechters die vooraf toezicht houden, onderzoeken "in their everyday practice" niet of er een redelijk vermoeden bestaat dat iemand bijvoorbeeld terroristische plannen heeft, en ze gaan ook niet na of het aftappen noodzakelijk en proportioneel is.[16]

Het Hof stelt ook vast dat het toezicht op de uitvoering van het aftappen in Rusland ineffectief is, onder meer omdat de Russische veiligheidsdienst technisch in staat is om alle mobiele communicatie direct te onderscheppen (denk ook aan hacken door de politie of geheime diensten: dit gebeurt buiten medewerking van de internetprovider om). Aangezien Ministeriële Verordening nr. 70 netwerkproviders verbiedt om bij te houden wanneer de dienst op die manier informatie verzamelt, heeft een toezichthouder geen zicht op de gevallen waarin de veiligheidsdienst niet volgens de regels een rechterlijke tapmacht heeft aangevraagd.[17] Het Hof veroordeelt in het bijzonder het toezicht in dit stadium door de Russische officier van justitie, omdat hij niet onafhankelijk lijkt te zijn van de regering,[18] niet de bevoegdheid heeft om te bevelen dat onrechtmatig onderschept materiaal vernietigd wordt,[19] en omdat aftappen in het kader van contraspionage *de facto* aan zijn toezicht ontsnapt.[20]

Met betrekking tot de effectiviteit van het toezicht achteraf, herhaalt het Hof in *Roman Zakharov* het belang van kennisgeving en informatieverstrekking aan de betrokkene. Iemand heeft namelijk alleen toegang tot de rechter of een klachtenprocedure bij een andere toezichthouder als ze weet dat ze is afgetapt. In *Klass en Anderen* formuleerde het Hof de regel dat kennisgeving aan de betrokkene in beginsel moet plaatsvinden zodra dit mogelijk is zonder het eigenlijke doel van de geheime surveillance op het spel te zetten. Het Hof merkt op dat betrokkenen in Rusland nooit geïnformeerd worden, en dat zij niet op andere zinvolle wijze informatie kunnen opvragen.[21] Deze twee factoren, en allerlei andere gebrekkige aspecten van de vier verschillende juridische procedures die afgetapte personen in theorie kunnen doorlopen, leiden tot het oordeel dat het Russische recht geen effectieve rechtsmiddelen ter beschikking stelt aan burgers die zijn afgetapt.[22] Het recht op privacy in artikel 8 EVRM impliceert nog geen "right to be informed" over geheime surveillance, maar volgens sommigen gaat het Hof met haar uitspraak in *Roman Zakharov* wel die kant op.[23]

### 5. *Hoe zit het nu met bulk interceptie?*

Uiteindelijk concludeert het Hof dat het Russische juridische kader voor het onderscheppen van mobiel telefoonverkeer in zijn geheel niet voorziet in effectieve waarborgen tegen willekeurigheid en machtsmisbruik,[24] en dat deze tekortkomingen doorwerken in de manier waarop de bevoegdheden in de praktijk worden uitgeoefend.[25] Net zoals het Hof van Justitie van de Europese Unie ("HvJ EU") in de zaken *Digital Rights Ireland*[26] en *Schrems*,[27] is het Straatsburgse Hof zeer kritisch over het onderscheppen en opslaan van telefoon- en internetverkeer, en toetst het wettelijk kader in zijn geheel. Het Hof stelt vast dat er een schending was van artikel 8 EVRM.[28]

9 Par. 231 *Roman Zakharov*.
10 Par. 232 *Roman Zakharov*.
11 Par. 233 *Roman Zakharov*.
12 Par. 234 *Roman Zakharov*.
13 Zie bijvoorbeeld de ontvankelijkheidsbeslissing in EHRM 29 juni 2006, 54934/00 (*Weber en Saravia/Duitsland)* en belangrijke surveillance zaken als *Weber en Saravia/Duitsland* en EHRM 18 mei 2010, 26839/05 (*Kennedy/Verenigd Koninkrijk*).
14 Zie par. 284 en 295 *Roman Zakharov*.
15 Par. 249 *Roman Zakharov*.
16 Par. 263 *Roman Zakharov*. Dit maakt het Hof op uit aantekeningen die de rechters zelf maakten, en uit statische informatie over het aantal keer dat de Russische geheime diensten een rechterlijke machtiging aanvroegen voor aftappen, en het percentage aanvragen (tussen de 93 en 99%) dat werd toegewezen.
17 Par. 272 *Roman Zakharov*.
18 Par. 279-280 *Roman Zakharov*.
19 Par. 282 *Roman Zakharov*.
20 Par. 281 *Roman Zakharov*.
21 Par. 289-290 *Roman Zakharov*.
22 Par. 291-300 *Roman Zakharov*.
23 Paul de Hert en Pedro Cristobal Bocos, 'Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment', *Strasbourg Observers*, 23 december 2015, http://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/ (laatst geraadpleegd 7 mei 2016).
24 Par. 302 *Roman Zakharov*.
25 Par. 303 *Roman Zakharov*.
26 HvJ EU 8 april 2014, in de gevoegde zaken van C-293/12 en C-594/12 (*Digital Rights Ireland)*, *Computerrecht* 2014-3, m.nt. R. van den Hoven van Genderen.
27 HvJ EU 6 oktober 2015, C-362/14 (*Schrems*), *Computerrecht* 2016-1, m.nt. G. Fruy.
28 Par. 305 *Roman Zakharov*.

*Roman Zakharov* gaat niet over het in bulk aftappen van elektronische communicatie,[29] maar het Hof suggereert wel dat grootschalige, niet-geïndividualiseerde surveillance niet te rechtvaardigen is onder het EVRM. Het Hof stelt namelijk dat de instantie die toestemming geeft voor geheime surveillance (i.e. voorafgaand toezicht) "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."[30] Het Hof stelt vast dat de Russische rechters die het tappen machtigen niet verplicht zijn om zo'n redelijk vermoeden te toetsen, of een noodzakelijkheid- en proportionaliteitstoets toe te passen,[31] en dat ze dit in de dagelijkse praktijk waarschijnlijk ook niet doen.[32]

Daarnaast stelt het Hof dat een tapmachtiging "must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information."[33] In sommige gevallen vereist Russische aftapwetgeving dat een tapmachtiging een specifiek persoon aanwijst, maar in andere gevallen is dit niet vereist. Het gevolg is dat rechters soms een machtiging afgeven om alle mobiele telefonie af te tappen in een gebied waar een misdrijf is gepleegd.[34] Het Hof zegt niet dat dit per definitie in strijd is met het EVRM, maar merkt wel op dat deze bepalingen een zeer ruime bevoegdheid geven aan de autoriteiten.[35] Bij bulk interceptie wordt een grote hoeveelheid elektronische communicatie en metadata opgevangen (bijvoorbeeld álle data die over een glasvezelkabel loopt), zonder dat er op bepaalde personen, objecten, of zoektermen wordt geselecteerd. Het is moeilijk in te zien hoe er in dat geval sprake kan zijn van "a reasonable suspicion" jegens een persoon (zie hierboven), en een machtiging die "a specific person … or a single set of premises" aanduidt.

Een maand na *Roman Zakharov* concludeert de gewone Kamer van het Hof in *Szabó en Vissy/Hongarije* dat Hongaarse wetgeving voor massale surveillance in strijd is met artikel 8 EVRM. In deze zaak klaagden verzoekers over de bevoegdheid van de Hongaarse veiligheidsdienst om ter bescherming van de nationale veiligheid brieven te lezen, elektronische communicatie te onderscheppen, en computers of netwerken te hacken. Als de veiligheidsdienst bij de minister toestemming vraagt om te surveilleren, moet de dienst betrokkenen bij naam aangeven, of "as a range of persons." Het Hof merkt op dat "a range of persons" op iedereen betrekking kan hebben, en de weg vrijmaakt voor onbegrensde surveillance van grote groepen burgers.[36] Het Hof overweegt dat de beklaagde regels strategische, grootschalige interceptie mogelijk maken, en vindt dit een serieus probleem.[37] Daar voegt het Hof aan toe dat het profileren van burgers door de overheid in het bijzonder een vergaande inmenging met het privéleven kan opleveren.[38] Toch berust de finale conclusie van het Hof dat artikel 8 EVRM is geschonden met name op de constatering dat de toestemming van de minister tekortschiet (hij toetst proportionaliteit en noodzakelijkheid onvoldoende) en het toezicht in Hongarije zwak is.[39]

De vraag is nu of *Roman Zakharov* en *Szabó en Vissy* betekenen dat massale surveillance per definitie in strijd is met het EVRM. Aan de ene kant wijzen de hierboven geciteerde passages in die richting.[40] Het Hof bepaalt in *Szabó en Vissy* ook (voor het eerst) dat "[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."[41]

Aan de andere kant kan de uitspraak van het Hof in *Szabó en Vissy* ook betekenen dat massale surveillance gerechtvaardigd is onder het EVRM, als het juridische kader ervoor voldoet aan de eisen die het Hof stelt (o.a. waarborgen in de wet en toezicht).[42] De *concurring opinion* bij *Szabó en Vissy* concludeert ook dat "[i]n practice, the Chamber condones *volenti nolenti* widespread, non-(reasonable) suspicion-based, 'strategic surveillance' for the purposes of national security (...)."[43] Er zijn drie verzoeken aanhangig bij het EHRM met betrekking tot bulk interceptie door het Verenigd Koninkrijk.[44] Misschien wordt in die zaken duidelijk of het Hof principieel stelling neemt tegen massale surveillance, of het onder omstandigheden toestaat.

*S.J. Eskens*

29 *Weber en Saravia/Duitsland*, *Liberty en Anderen/Verenigd Koninkrijk*, en *Szabó en Vissy/Hongarije* (zie hieronder) gaan wel over bulk interceptie.
30 Par. 260 *Roman Zakharov*.
31 Par. 262 *Roman Zakharov*.
32 Par. 263 *Roman Zakharov*.
33 Par. 264 *Roman Zakharov*.
34 Par. 265 *Roman Zakharov*.
35 Par. 265 *Roman Zakharov*.
36 EHRM 12 januari 2016, 37138/14 (*Szabó en Vissy/Hongarije*), par. 67.
37 Par. 69 *Szabó en Vissy*.
38 Par. 70 *Szabó en Vissy*.
39 Par. 89 *Szabó en Vissy*. Zie ook hoe het Hof eerst ingaat op het problematische karakter van grootschalige interceptie, maar vervolgens besluit dat "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 [die het Hof ook in *Roman Zakharov* aanhaalde]" (par. 70). Daarmee lijkt het Hof de cruciale vraag nog even uit te stellen.
40 Zie ook Carly Nyst, 'European Human Rights Court Deals a Heavy Blow to the Lawfulness of Bulk Surveillance', *Just Security*, 9 december 2015, https://www.justsecurity.org/28216/echr-deals-heavy-blow-lawfulness-bulk-surveillance/ (laatst geraadpleegd 7 mei 2016).
41 Par. 73 *Szabó en Vissy*.
42 Zie voor een vergelijkbare analyse van recente rechtspraak van het HvJ EU Frederik J. Zuiderveen Borgesius en Axel Arnbak, 'New Data Security Requirements and the Proceduralization of Mass Surveillance Law after the European Data Retention Case', *Amsterdam Law School Research Paper No. 2015-41*, verkrijgbaar op http://ssrn.com/abstract=2678860.
43 Pagina 66 *Szabó en Vissy*.
44 Zie de verzoeken aanhangig gemaakt bij het EHRM op 4 september 2013, 58170/13 (*Big Brother Watch en Anderen/Verenigd Koninkrijk*), 11 september 2014, 62322/14 (*Bureau of Investigative Journalism en Alice Ross/Verenigd Koninkrijk*), en 20 mei 2015, 24960/15 (*10 Mensenrechtenorganisaties en Anderen/Verenigd Koninkrijk*).