NJ 2017/185

EUROPEES HOF VOOR DE RECHTEN VAN DE MENS
4 december 2015, nr. 47143/06
(D. Spielmann, J. Casadevall, G. Raimondi, I. Ziemele, M. Villiger, L. López Guerra, K. Hajiyev, A. Nußberger, J. Laffranque, L.-A. Sicilianos, E. Møse, A. Potocki, P. Lemmens, H. Jäderblom, F. Vehabović, K. Turković, D. Dedov)
m.nt. E.J. Dommering

Art. 8 EVRM

Computerrecht 2016/86
NJB 2016/402
ECLI:CE:ECHR:2015:1204JUD004714306

Russische wet- en regelgeving verplicht telecomproviders apparatuur te installeren die veiligheidsdiensten onbeperkte toegang verschaft tot telefoonverkeer. Vereiste van 'quality of law'; beperking van heimelijke onderscheppingen tot hetgeen noodzakelijk is in een democratische samenleving? Schending art. 8 EVRM.

Verzoeker is hoofdredacteur van een uitgeverij en een tijdschrift en tevens voorzitter van een NGO die zich toelegt op de bescherming van de persvrijheid. In een door hem tegen een drietal telecomproviders geëntameerde procedure heeft hij zich op het standpunt gesteld dat sprake is van een inmenging in zijn recht op eerbiediging van de privacy van zijn telefoonverkeer. Volgens verzoeker hebben de telecomproviders ter naleving van Russische wet- en regelgeving apparatuur geïnstalleerd die de veiligheidsdiensten in staat stelt al het telefoonverkeer te onderscheppen zonder voorafgaande rechterlijke machtiging. Zijn vorderingen zijn in nationale instanties afgewezen, onder meer omdat hij niet bewezen zou hebben dat zijn telefoonverkeer is onderschept en omdat het enkel installeren van apparatuur geen inmenging zou opleveren.

Ten overstaan van het EHRM klaagt verzoeker dat het Russische stelsel van heimelijke onderschepping van telefoonverkeer niet voldoet aan de eisen van art. 8 EVRM.

EHRM: Verzoeker behoeft niet aan te tonen dat hij het risico loopt onderschept te worden, aangezien het door de bestreden wet- en regelgeving gecreëerde systeem van heimelijke onderscheppingen alle gebruikers van de relevante telecomproviders treft (r.o. 152-179). De bestreden wet- en regelgeving voorziet niet in adequate en effectieve waarborgen tegen willekeur en het inherente misbruikrisico. In het bijzonder is onvoldoende duidelijk omschreven in welke gevallen en gedurende welke periode de autoriteiten bevoegd zijn tot de heimelijke onderscheppingen dan wel hoe de verzamelde data worden opgeslagen en vernietigd, biedt de rechterlijke toetsing onvoldoende waarborgen omdat daarbij de noodzakelijkheid en proportionaliteit niet worden getoetst, is het uitgeoefende toezicht onvoldoende om effectieve en doorlopende controle te verzekeren en wordt de effectiviteit van de beschikbare rechtsmiddelen ondermijnd door het ontbreken van enige kennisgeving aan de betrokkene (r.o. 180-305).

Zakharov
tegen
Rusland

EHRM:

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

A. Admissibility

Enz. (*red.*)

B. Merits

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

(a) Submissions by the parties

(i) The Government

152. The Government submitted that the applicant could not claim to be a victim of the alleged violation of Article 8 of the Convention and that there had been no interference with his rights. He had not complained that his communications had been intercepted. The gist of his complaint before the domestic courts and the Court was that communications service providers had installed special equipment enabling the authorities to perform operational-search activities. In the Government's opinion, the case of *Orange Slovensko, A. S. v. Slovakia* ((dec.), no. 43983/02, 24 October 2006) confirmed that installation of interception equipment, or even its financing, by private companies was not in itself contrary to the Convention.

153. The Government further submitted that Article 34 could not be used to lodge an application in the nature of an *actio popularis*; nor could it form the basis of a claim made *in abstracto* that a law contra-

vened the Convention (they referred to *Aalmoes and 112 Others v. the Netherlands* (dec.), no. 16269/02, 25 November 2004). They argued that the approach to victim status established in the cases of *Klass and Others v. Germany* (6 September 1978, § 34, Series A no. 28) and *Malone v. the United Kingdom* (2 August 1984, § 64, Series A no. 82) — according to which an individual might, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him or her — could not be interpreted so broadly as to encompass every person in the respondent State who feared that the security services might have compiled information about him or her. An applicant was required to demonstrate that there was a 'reasonable likelihood' that the security services had compiled and retained information concerning his or her private life (they referred to *Esbester v. the United Kingdom*, no. 18601/91, Commission decision of 2 April 1993; *Redgrave v. the United Kingdom*, no. 20271/92, Commission decision of 1 September 1993; *Matthews v. the United Kingdom*, no. 28576/95, Commission decision of 16 October 1996; *Halford v. the United Kingdom*, 25 June 1997, § 17, Reports of Judgments and Decisions 1997-III; *Weber and Saravia v. Germany* (dec.), no. 54934/00, §§ 4-6 and 78, ECHR 2006-XI; and *Kennedy v. the United Kingdom*, no. 26839/05, §§ 122 and 123, 18 May 2010).

154. The Government maintained that exceptions to the rule of 'reasonable likelihood' were permissible only for special reasons. An individual could claim an interference as a result of the mere existence of legislation permitting secret surveillance measures in exceptional circumstances only, having regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him or her (they cited *Kennedy*, cited above, § 124). According to the Government, no such special reasons could be established in the present case.

155. Firstly, there was no 'reasonable likelihood', or indeed any risk whatsoever, that the applicant had been subjected to surveillance measures because he had not been suspected of any criminal offences. The fact that he was the editor-in-chief of a publishing company could not serve as a ground for interception under Russian law. The Government asserted that the applicant's telephone conversations had never been intercepted. The applicant had not produced any proof to the contrary. The documents submitted by him in the domestic proceedings had concerned third persons and had not contained any proof that his telephone had been tapped.

156. Secondly, remedies were available at the national level to challenge both the alleged insufficiency of safeguards against abuse in Russian law and any specific surveillance measures applied to an individual. It was possible to request the Constitutional Court to review the constitutionality of the OSAA. It was also possible to lodge a complaint with the Supreme Court, as had been successfully done by Mr N., who had obtained a finding of unlawfulness in respect of a provision of the Ministry of Communications' Order no. 130 (…). As regards Order no. 70, contrary to the applicant's allegations, it had been duly published (see paragraph 181 below) and could therefore be challenged in courts. A person whose communications had been intercepted unlawfully without prior judicial authorisation could also obtain redress in a civil court. The Government referred to the Supreme Court's judgment of 15 July 2009, which found that the installation of a video camera in the claimant's office and the tapping of his office telephone had been unlawful because those surveillance measures had been carried out without prior judicial authorisation (see also paragraphs 219 to 224 below). Finally, Russian law provided for supervision of interception of communications by an independent body, the prosecutor's office.

157. The Government concluded, in view of the above, that the present case was different from the case of *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (no. 62540/00, 28 June 2007) where the Court had refused to apply the 'reasonable likelihood' test because of the absence of any safeguards against unlawful interception in Bulgaria. Given that Russian law provided for adequate and sufficient safeguards against abuse in the sphere of interception of communications, including available remedies, in the Government' opinion, the applicant could not claim an interference as a result of the mere existence of legislation permitting secret surveillance. In the absence of a 'reasonable likelihood' that his telephone communications had been intercepted, he could not claim to be a victim of the alleged violation of Article 8 of the Convention.

(ii) The applicant

158. The applicant submitted that he could claim to be a victim of a violation of Article 8 occasioned by the mere existence of legislation which allowed a system of secret interception of communications, without having to demonstrate that such secret measures had been in fact applied to him. The existence of such legislation entailed a threat of surveillance for all users of the telecommunications services and therefore amounted in itself to an interference with the exercise of his rights under Article 8. He relied in support of his position on the cases of *Klass and Others* (cited above, §§ 34 and 37), *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, § 58) and *Kennedy* (cited above, § 123).

159. The applicant maintained that the test of 'reasonable likelihood' had been applied by the Court only in those cases where the applicant had alleged actual interception, while in the cases concerning general complaints about legislation and practice permitting secret surveillance measures

the 'mere existence' test established in the *Klass and Others* judgment had been applied (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 59, and *Kennedy*, cited above, §§ 122 and 123, with further references). In the case of *Liberty and Others v. the United Kingdom* (no. 58243/00 [*NJ* 2010/324, m.nt. E.J. Dommering; *red.*], §§ 56 and 57, 1 July 2008), the Court found that the existence of powers permitting the authorities to intercept communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied. In the case of *Kennedy* (cited above, § 124) that test had been further elaborated to include the assessment of availability of any remedies at the national level and the risk of secret surveillance measures being applied to the applicant. Finally, in the case of *Mersch and Others v. Luxemburg* (nos. 10439/83 et al., Commission decision of 10 May 1985) the Commission found that in those cases where the authorities had no obligation to notify the persons concerned about the surveillance measures to which they had been subjected, the applicants could claim to be 'victims' of a violation of the Convention on account of the mere existence of secret surveillance legislation, even though they could not allege in support of their applications that they had been subjected to an actual measure of surveillance.

160. The applicant argued that he could claim to be a victim of a violation of Article 8, on account both of the mere existence of secret surveillance legislation and of his personal situation. The OSAA, taken together with the FSB Act, the Communications Act and the Orders adopted by the Ministry of Communication, such as Order no. 70, permitted the security services to intercept, through technical means, any person's communications without obtaining prior judicial authorisation for interception. In particular, the security services had no obligation to produce the interception authorisation to any person, including the communications service provider. The contested legislation therefore permitted blanket interception of communications.

161. No remedies were available under Russian law to challenge that legislation. Thus, as regards the possibility to challenge Order no. 70, the applicant referred to the Supreme Court's decision of 25 September 2000 on a complaint by a Mr N. (…) finding that that Order was technical rather than legal in nature and was therefore not subject to official publication. He also submitted a copy of the decision of 24 May 2010 by the Supreme Commercial Court finding that the Orders by the Ministry of Communications requiring communications providers to install equipment enabling the authorities to perform operational-search activities were not subject to judicial review in commercial courts. The domestic proceedings brought by the applicant had shown that Order no. 70 could not be effectively challenged before Russian courts. Further, as far as the OSAA was concerned, the Constitutional Court had already examined its constitutionality on a number of occasions and had found that it was compatible with the Constitution. Finally, as regards the possibility to challenge individual surveillance measures, the applicant submitted that the person concerned was not notified about the interception, unless the intercepted material had been used as evidence in criminal proceedings against him. In the absence of notification, the domestic remedies were ineffective (see also paragraph 217 below).

162. As to his personal situation, the applicant submitted that he was a journalist and the chairperson of the St Petersburg branch of the Glasnost Defence Foundation, which monitored the state of media freedom and provided legal support to journalists whose professional rights had been violated (…). His communications were therefore at an increased risk of being intercepted. The applicant referred in that connection to the fundamental importance of protecting journalists' sources, emphasised by the Grand Chamber judgment in *Sanoma Uitgevers B.V. v. the Netherlands* ([GC], no. 38224/03 [*NJ* 2011/230 m.nt. E.J. Dommering en T.M. Schalken], § 50, 14 September 2010).

(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

164. The Court has consistently held in its case-law that the Convention does not provide for the institution of an *actio popularis* and that its task is not normally to review the relevant law and practice *in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention (see, among other authorities, *N.C. v. Italy* [GC], no. 24952/94, § 56, ECHR 2002-X; *Krone Verlag GmbH & Co. KG v. Austria (no. 4)*, no. 72331/01 [*NJ* 2008/433, m.nt. E.J. Dommering], § 26, 9 November 2006; and *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], no. 47848/08, § 101, ECHR 2014). Accordingly, in order to be able to lodge an application in accordance with Article 34, an individual must be able to show that he or she was 'directly affected' by the measure complained of. This is indispensable for putting the protection mechanism of the Convention into motion, although this criterion is not to be applied in a rigid, mechanical and inflexible way throughout the proceedings (see *Centre for Legal Resources on behalf of Valentin Câmpeanu,* cited above, § 96).

165. Thus, the Court has permitted general challenges to the relevant legislative regime in the sphere of secret surveillance in recognition of the par-

ticular features of secret surveillance measures and the importance of ensuring effective control and supervision of them. In the case of *Klass and Others v. Germany* the Court held that an individual might, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him. The relevant conditions were to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures (see *Klass and Others,* cited above, § 34). The Court explained the reasons for its approach as follows:

"36. The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8, or even to be deprived of the right granted by that Article, without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions … The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25 [currently Article 34], since otherwise Article 8 runs the risk of being nullified.

37. As to the facts of the particular case, the Court observes that the contested legislation institutes a system of surveillance under which all persons in the Federal Republic of Germany can potentially have their mail, post and telecommunications monitored, without their ever knowing this unless there has been either some indiscretion or subsequent notification in the circumstances laid down in the Federal Constitutional Court's judgment … To that extent, the disputed legislation directly affects all users or potential users of the postal and telecommunication services in the Federal Republic of Germany. Furthermore, as the Delegates rightly pointed out, this 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 …

38. Having regard to the specific circumstances of the present case, the Court concludes that each of the applicants is entitled to '(claim) to be the victim of a violation' of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance. The question whether the applicants were actually the victims of any violation of the Convention involves determining whether the contested legislation is in itself compatible with the Convention's provisions …"

166. Following the *Klass and Others* case, the case-law of the Convention organs developed two parallel approaches to victim status in secret surveillance cases.

167. In several cases the Commission and the Court held that the test in *Klass and Others* could not be interpreted so broadly as to encompass every person in the respondent State who feared that the security services might have compiled information about him or her. An applicant could not, however, be reasonably expected to prove that information concerning his or her private life had been compiled and retained. It was sufficient, in the area of secret measures, that the existence of practices permitting secret surveillance be established and that there was a reasonable likelihood that the security services had compiled and retained information concerning his or her private life (see *Esbester,* cited above; *Redgrave,* cited above; *Christie v. the United Kingdom*, no. 21482/93, Commission decision of 27 June 1994; *Matthews,* cited above; *Halford,* cited above, §§ 47 and 55-57; and *Iliya Stefanov v. Bulgaria*, no. 65755/01, §§ 49 and 50, 22 May 2008). In all of the above cases the applicants alleged actual interception of their communications. In some of them they also made general complaints about legislation and practice permitting secret surveillance measures (see *Esbester, Redgrave, Matthews,* and *Christie*, all cited above).

168. In other cases the Court reiterated the *Klass and Others* approach that the mere existence of laws and practices which permitted and established a system for effecting secret surveillance of communications entailed a threat of surveillance for all those to whom the legislation might be applied. This threat necessarily affected freedom of communication between users of the telecommunications services and thereby amounted in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (see *Malone,* cited above, § 64; *Weber and Saravia,* cited above, § 78; *Association for European Integration and Human Rights and Ekimdzhiev,* cited above, §§ 58, 59 and 69; *Liberty and Others,* cited above, §§ 56 and 57; and *Iordachi and Others v. Moldova*, no. 25198/02, §§ 30-35, 10 February 2009). In all of the above cases the applicants made general complaints about legislation and practice permitting secret surveillance measures. In some of them they also alleged actual interception of their communications (see *Malone,* cited above, § 62; and *Liberty and Others,* cited above, §§ 41 and 42).

169. Finally, in its most recent case on the subject, *Kennedy v. the United Kingdom,* the Court held

that sight should not be lost of the special reasons justifying the Court's departure, in cases concerning secret measures, from its general approach which denies individuals the right to challenge a law *in abstracto*. The principal reason was to ensure that the secrecy of such measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court. In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him or her. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court (see *Kennedy*, cited above, § 124).

(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).

174. 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 secret surveillance measures and a risk of being subjected to such measures, rather than as a result of any specific surveillance measures applied to him.

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

(a) Submissions by the parties

(i) Accessibility of domestic law

180. The applicant submitted that the addendums to Order no. 70 describing the technical requirements for the equipment to be installed by communications service providers had never been officially published and were not accessible to the public. In the applicant's opinion, in so far as they determined the powers of the law-enforcement authorities with regard to secret surveillance, they affected citizens' rights and ought therefore to have been published. The fact that the applicant had eventually had access to the addendums in the domestic proceedings could not remedy the lack of an official publication (he referred to *Kasymakhunov and Saybatalov v. Russia*, nos. 26261/05 and 26377/06, § 92, 14 March 2013). Citizens should not be required to engage judicial proceedings to obtain access to regulations applicable to them. The Court had already found that it was essential to have clear, detailed and accessible rules on the application of secret measures of surveillance (*Shimovolos v. Russia*, no. 30194/09, § 68, 21 June 2011).

181. The Government submitted that Order no. 70 was technical in nature and was not therefore subject to official publication. It had been published in a specialised magazine, *SvyazInform,* in issue no. 6 of 1999. It was also available in the *ConsultantPlus* internet legal database, and was accessible without charge. The applicant had submitted a copy of the Order with its addendums to the Court, which showed that he had been able to obtain access to it. The domestic law was therefore accessible.

(ii) Scope of application of secret surveillance measures

182. The applicant submitted that the Court had already found that the OSAA did not meet the 'foreseeability' requirement because the legal discretion of the authorities to order 'an operative experiment' involving recording of private communications through a radio-transmitting device was not subject to any conditions, and the scope and the manner of its exercise were not defined (see *Bykov v. Russia* [GC], no. 4378/02, § 80, 10 March 2009). The present case was similar to the *Bykov* case. In particular, Russian law did not clearly specify the categories of persons who might be subjected to interception measures. In particular, surveillance measures were not limited to persons suspected or accused of criminal offences. Any person who had information about a criminal offence could have his or her telephone tapped. Furthermore, interception was not limited to serious and especially serious offences. Russian law allowed interception measures in connection with offences of medium severity, such as, for example, pickpocketing.

183. The Government submitted that interception of communications might be conducted only following the receipt of information that a criminal offence had been committed or was ongoing, or was being plotted; about persons conspiring to commit, or committing, or having committed a criminal offence; or about events or activities endangering the national, military, economic or ecological security of the Russian Federation. The Constitutional Court had held in its ruling of 14 July 1998 that collecting information about a person's private life was permissible only with the aim of preventing, detecting and investigating criminal offences or in pursuance of other lawful aims listed in the OSAA.

184. Only offences of medium severity, serious offences and especially serious offences might give rise to an interception order and only persons suspected of such offences or who might have information about such offences could be subject to interception measures. The Government submitted in this connection that the Court had already found that surveillance measures in respect of a person who was not suspected of any offence could be justified under the Convention (see *Greuter v. the Netherlands* (dec.), no. 40045/98, 19 March 2002).

185. Further, in respect of interceptions for the purposes of protecting national security, the Government argued that the requirement of 'foreseeability' of the law did not go so far as to compel States to enact legal provisions listing in detail all conduct that might prompt a decision to subject an individual to surveillance on 'national security' grounds (see *Kennedy*, cited above, § 159).

(iii) The duration of secret surveillance measures

186. The applicant submitted that the OSAA did not explain under which circumstance interception could be extended beyond six months. Nor did it establish the maximum duration of interception measures.

187. The Government submitted that under Russian law interception might be authorised by a judge for a maximum period of six months and might be extended if necessary. It had to be discontinued if the investigation was terminated. They argued that it was reasonable to leave the duration of the interception to the discretion of the domestic authorities, having regard to the complexity and the duration of the investigation in a specific case

(see *Kennedy*, cited above). They also referred to the case of *Van Pelt v. the Netherlands* (no. 20555/92, Commission decision of 6 April 1994), where the Commission had found that the tapping of the applicant's telephone for almost two years had not violated the Convention.

(iv) Procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data

188. The applicant further submitted that the OSAA did not specify the procedures to be followed for examining, storing, accessing or using the intercept data or the precautions to be taken when communicating the data to other parties. It provided that the data had to be destroyed within six months, unless that data were needed in the interest of the service or of justice. There was however no definition of what the 'interest of the service or of justice' meant. Russian law also gave complete freedom to the trial judge as to whether to store or to destroy data used in evidence after the end of the trial.

189. The Government submitted that the OSAA required that records of intercepted communications had to be stored under conditions excluding any risk of their being listened to or copied by unauthorised persons. The judicial decision authorising interception of communications, the materials that served as a basis for that decision and the data collected as result of interception constituted a State secret and were to be held in the exclusive possession of the State agency performing interceptions. If it was necessary to transmit them to an investigator, a prosecutor or a court, they could be declassified by the heads of the agencies conducting operational-search activities. Interception authorisations were declassified by the courts which had issued them. The procedure for transmitting the data collected in the course of operational-search activities to the competent investigating authorities or a court was set out in the Ministry of the Interior's Order of 27 September 2013 (…).

190. The data collected in the course of operational-search activities were to be stored for one year and then destroyed, unless it was needed in the interests of the service or of justice. Recordings were to be stored for six months and then destroyed. Russian law was therefore foreseeable and contained sufficient safeguards.

(v) Authorisation of secret surveillance measures

(α) The applicant

191. The applicant submitted that although domestic law required prior judicial authorisation for interceptions, the authorisation procedure did not provide for sufficient safeguards against abuse. Firstly, in urgent cases communications could be intercepted without judicial authorisation for up to forty-eight hours. Secondly, in contrast to the CCrP, the OSAA did not provide for any requirements concerning the content of the interception authorisation. In particular, it did not require that the interception subject be clearly specified in the authorisation by name, telephone number or address (see, by contrast, the United Kingdom's and Bulgarian legislation reproduced in *Kennedy*, cited above, §§ 41 and 160; and *Association for European Integration and Human Rights and Ekimdzhiev,* cited above, § 13). Nor did domestic law require that the authorisation specify which communications, or types of communications, should be recorded in order to limit the law-enforcement authorities' discretion to determine the scope of surveillance measures. Russian law did not establish any special rules for surveillance in sensitive situations, for example where the confidentiality of journalists' sources was at stake, or where surveillance concerned privileged lawyer-client communications.

192. The applicant further submitted that the domestic law did not impose any requirement on the judge to verify the existence of a 'reasonable suspicion' against the person concerned or to apply the 'necessity' and 'proportionality' test. The requesting authorities had no obligation to attach any supporting materials to the interception requests. Moreover, the OSAA expressly prohibited submission to the judge of certain materials — those containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures — thereby making it impossible for the judge to effectively verify the existence of a 'reasonable suspicion'. Russian law did not require that the judge should authorise interception only when it was impossible to achieve the legitimate aims by other less intrusive means.

193. In support of his allegation that the judges did not verify the existence of a 'reasonable suspicion' against the person concerned and did not apply the 'necessity' and 'proportionality' test, the applicant produced copies of analytical notes issued by three District Courts in different Russian regions (the Tambov region, the Tula region and the Dagestan Republic). The courts summarised their own case-law concerning operational-search measures involving interference with the privacy of communications or privacy of the home for the period from 2010 to 2013. One of the courts noted that it refused authorisation to carry out an operational-search measure if it did not appear on the list of operational-search measures in the OSAA, if the request for authorisation was not signed by a competent official or was not reasoned, or if the case fell under statutory restrictions on the use of that measure (for example, relating to the person's status or to the nature of the offence). Authorisation was given if all of the above conditions were met. Another court stated that authorisation could also be refused if the request was insufficiently reasoned, that is, if it did not contain sufficient information permitting the judge to ascertain that the measure was lawful and justified. The third court stated that it granted authorisation if that was requested by the law-enforcement authorities. It never refused a request for

authorisation. All three courts considered that the request was sufficiently reasoned if it referred to the existence of information listed in section 8(2) of the OSAA (…). One of the courts noted that supporting materials were never attached to requests for authorisation; another court noted that some, but not all, of the requests were accompanied by supporting materials, while the third court stated that all requests were accompanied by supporting materials. In all three courts the judges never requested the law-enforcement authorities to submit additional supporting materials, such as materials confirming the grounds for the interception or proving that the telephone numbers to be tapped belonged to the person concerned. Two courts granted interception authorisations in respect of unidentified persons, one of them specifying that such authorisations only concerned collection of data from technical channels of communication. Such authorisations did not mention a specific person or a telephone number to be tapped, but authorised interception of all telephone communications in the area where a criminal offence had been committed. One court never gave such authorisations. Two courts noted that authorisations always indicated the duration for which the interception was authorised, while one court stated that the duration of interception was not indicated in the authorisations issued by it. Finally, none of the three courts had examined any complaints from persons whose communications had been intercepted.

194. The applicant also produced official statistics by the Supreme Court for the period from 2009 to 2013. It could be seen from those statistics that in 2009 Russian courts granted 130,083 out of 132,821 requests under the CCrP and 245,645 out of 246,228 requests under the OSAA (99%). In 2010 the courts allowed 136,953 out of 140,372 interception requests under the CCrP and 276,682 out of 284,137 requests under the OSAA. In 2011 the courts allowed 140,047 out of 144,762 interception requests under the CCrP and 326,105 out of 329,415 requests under the OSAA. In 2012 they granted 156,751 out of 163,469 interception requests under the CCrP (95%) and 372,744 out of 376,368 requests under the OSAA (99%). In 2013 the courts allowed 178,149 out of 189,741 interception requests lodged under the CCrP (93%) and 416,045 out of 420,242 interception requests lodged under the OSAA (99%). The applicant drew the Court's attention to the fact that the number of interception authorisations had almost doubled between 2009 and 2013. He also argued that the very high percentage of authorisations granted showed that the judges did not verify the existence of a 'reasonable suspicion' against the interception subject and did not exercise careful and rigorous scrutiny. As a result interceptions were ordered in respect of vast numbers of people in situations where the information could have been obtained by other less intrusive means.

195. The applicant concluded from the above that the authorisation procedure was defective and was therefore not capable of confining the use of secret surveillance measures to what was necessary in a democratic society.

196. As regards safeguards against unauthorised interceptions, the applicant submitted that the law-enforcement authorities were not required under domestic law to show judicial authorisation to the communications service provider before obtaining access to a person's communications. All judicial authorisations were classified documents, kept in the exclusive possession of law-enforcement authorities. An obligation to forward an interception authorisation to the communications service provider was mentioned only once in Russian law in connection with monitoring of communications-related data under the CCrP (…). The equipment the communications service providers had installed pursuant to the Orders issued by the Ministry of Communications, in particular the unpublished addendums to Order No. 70, allowed the law-enforcement authorities direct and unrestricted access to all mobile telephone communications of all users. The communications service providers also had an obligation under Order no. 538 to create databases storing for three years information about all subscribers and the services provided to them. The secret services had direct remote access to those databases. The manner in which the system of secret surveillance thus operated gave the security services and the police technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation. The necessity to obtain prior judicial authorisation therefore arose only in those cases where the intercepted data had to be used as evidence in criminal proceedings.

197. The applicant produced documents showing, in his view, that law-enforcement officials unlawfully intercepted telephone communications without prior judicial authorisation and disclosed the records to unauthorised persons. For example, he produced printouts from the Internet containing transcripts of the private telephone conversations of politicians. He also submitted news articles describing criminal proceedings against several high-ranking officers from the police technical department. The officers were suspected of unlawfully intercepting the private communications of politicians and businessmen in return for bribes from their political or business rivals. The news articles referred to witness statements to the effect that intercepting communications in return for bribes was a widespread practice and that anyone could buy a transcript of another person's telephone conversations from the police.

(β) The Government

198. The Government submitted that any interception of telephone or other communications had to be authorised by a court. The court took a decision on the basis of a reasoned request by a law-enforcement authority. The burden of proof was on

the requesting authority to justify the necessity of the interception measures. To satisfy that burden of proof, the requesting authorities enclosed with their request all relevant supporting materials, except materials containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures. That exception was justified by the necessity to ensure the security and protection of undercover agents and police informers and their family members and was therefore compatible with the Convention.

199. The Government further referred to the Plenary Supreme Court's Ruling of 27 June 2013, which explained to the lower courts that any restrictions on human rights and freedoms had to be prescribed by law and be necessary in a democratic society, that is, proportionate to a legitimate aim. Courts were instructed to rely on established facts, verify the existence of relevant and sufficient reasons to justify a restriction on an individual's right and balance the interests of the individual whose rights were restricted against the interests of other individuals, the State and society. The OSAA explicitly required the courts to give reasons for the decision to authorise interception. In line with the Constitutional Court's decision of 8 February 2007 (…), the interception authorisation was to refer to the specific grounds for suspecting the person in respect of whom operational-search measures were requested of a criminal offence or of activities endangering national, military, economic or ecological security. In its decision of 2 October 2003 (…), the Constitutional Court also held that judges had an obligation to examine the materials submitted to them carefully and thoroughly.

200. According to the Government, in practice, each interception authorisation specified the State agency which was responsible for performing the interception, the grounds for conducting the surveillance measures and the reasons why they were necessary, a reference to applicable legal provisions, the person whose communications were to be intercepted, the grounds for suspecting that person's involvement in the commission of a specific criminal offence, that person's telephone number or IMEI code, the period of time for which the authorisation was granted and other necessary information. In exceptional circumstances it was permissible to authorise the interception of communications of unidentified persons. As a rule, in such cases a judge authorised the collection of data from technical channels of communication in order to identify the persons present at a specific location at the time that a criminal offence was committed there. That practice was compatible with the principles established in the Court's case-law, because in such cases the interception authorisation specified a single set of premises (locations) as the premises (locations) in respect of which the authorisation was ordered (they referred to *Kennedy*, cited above).

201. Russian law permitted communications to be intercepted without prior judicial authorisation in cases of urgency. A judge had to be informed of any such case within twenty-four hours and judicial authorisation for continuing the interception had to be obtained within forty-eight hours. According to the Government, the judge had to examine the lawfulness of such interception even in those cases when it had already been discontinued. They referred to an appeal judgment of 13 December 2013, in a criminal case in which the Supreme Court declared inadmissible as evidence recordings of telephone conversations obtained under the urgent procedure without prior judicial authorisation. The Supreme Court had held that although a judge had been informed about the interception, no judicial decision on its lawfulness and necessity had ever been issued.

(vi) Supervision of the implementation of secret surveillance measures

(α) The applicant

202. Regarding supervision of interceptions, the applicant argued at the outset that in Russia the effectiveness of any supervision was undermined by the absence of an obligation on the intercepting authorities to keep records of interceptions carried out by them. Moreover, Order no. 70 explicitly provided that information about interceptions could not be logged or recorded.

203. The applicant further submitted that in Russia neither the judge who had issued the interception authorisation nor any other independent official qualified for judicial office had power to supervise its implementation, and in particular to review whether the surveillance remained within the scope determined by the interception authorisation and complied with various requirements contained in domestic law.

204. Domestic law did not set out any procedures for the supervision of interceptions by the President, Parliament and the Government. They certainly had no powers to supervise the implementation of interception measures in specific cases.

205. As regards supervision by the Prosecutor General and competent low-level prosecutors, they could not be considered independent because of their position within the criminal justice system and their prosecuting functions. In particular, prosecutors gave their approval to all interception requests lodged by investigators in the framework of criminal proceedings and participated in the related court hearings. They could then use the data obtained as a result of the interception in the framework of their prosecuting functions, in particular by presenting it as evidence during a trial. There was therefore a conflict of interest with the prosecutor performing the dual function of a party to a criminal case and an authority supervising interceptions.

206. The applicant further submitted that the prosecutors' supervisory functions were limited because certain materials, in particular those revealing the identity of undercover agents or the tactics,

methods and means used by the security services, were outside the scope of their supervision. The prosecutors' supervisory powers were also limited in the area of counter-intelligence, where inspections could be carried out only following an individual complaint. Given the secrecy of interception measures and the lack of any notification of the person concerned, such individual complaints were unlikely to be lodged, with the result that counter-intelligence-related surveillance measures *de facto* escaped any supervision by prosecutors. It was also significant that prosecutors had no power to cancel an interception authorisation, to discontinue unlawful interceptions or to order the destruction of unlawfully obtained data.

207. Further, prosecutors' biannual reports were not published or publicly discussed. The reports were classified documents and contained statistical information only. They did not contain any substantive analysis of the state of legality in the sphere of operational-search activities or any information about what breaches of law had been detected and what measures had been taken to remedy them. Moreover, the reports amalgamated together all types of operational-search activities, without separating interceptions from other measures.

(β) The Government

208. The Government submitted that supervision of operational-search activities, including interceptions of telephone communications, was exercised by the President, the Parliament and the Government. In particular, the President determined the national security strategy and appointed and dismissed the heads of all law-enforcement agencies. There was also a special department within the President's Administration which supervised the activities of the law-enforcement agencies, including operational-search activities. That department consisted of officials from the Interior Ministry and the FSB who had the appropriate level of security clearance. Parliament participated in the supervision process by adopting and amending laws governing operational-search activities. It could also form committees and commissions and held parliamentary hearings on all issues, including those relating to operational-search activities, and could hear the heads of law-enforcement agencies if necessary. The Government adopted decrees and orders governing operational-search activities and allocated the budgetary funds to the law-enforcement agencies.

209. Supervision was also exercised by the Prosecutor General and competent low-level prosecutors who were independent from the federal, regional and local authorities. The Prosecutor General and his deputies were appointed and dismissed by the Federation Council, the upper house of Parliament. Prosecutors were not entitled to lodge interception requests. Such requests could be lodged either by the State agency performing operational-search activities in the framework of the OSAA, or by the investigator in the framework of the CCrP. The prosecutor could not give any instructions to the investigator. In the course of a prosecutor's inspection, the head of the intercepting agency had an obligation to submit all relevant materials to the prosecutor at his or her request and could be held liable for the failure to do so. The prosecutors responsible for supervision of operational-search activities submitted six-monthly reports to the Prosecutor General. The reports did not however analyse interceptions separately from other operational-search measures.

(vii) Notification of secret surveillance measures

(α) The applicant

210. The applicant further submitted that Russian law did not provide that a person whose communications had been intercepted was to be notified before, during or after the interception. He conceded that it was acceptable not to notify the person before or during the interception, since the secrecy of the measure was essential to its efficacy. He argued, however, that such notification was possible after the interception had ended, 'as soon as it could be made without jeopardising the purpose of the restriction' (he referred to *Klass and Others,* cited above). In Russia the person concerned was not notified at any point. He or she could therefore learn about the interception only if there was a leak or if criminal proceedings were opened against him or her, and the intercepted data were used in evidence.

211. With regard to the possibility of obtaining access to the data collected in the course of interception, the applicant submitted that such access was possible only in very limited circumstances. If criminal proceedings had never been opened or if the charges had been dropped on other grounds than those listed in the OSAA, the person concerned was not entitled to have access. Furthermore, before obtaining access, the claimant had to prove that his or her communications had been intercepted. Given the secrecy of the surveillance measures and the lack of notification, such burden of proof was impossible to satisfy unless the information about the interception had been leaked. Even after satisfying all those preconditions, the person could only receive 'information about the data collected' rather than obtain access to the data themselves. Finally, only information that did not contain State secrets could be disclosed. Given that under the OSAA all data collected in the course of operational-search activities constituted a State secret and the decision to declassify it belonged to the head of the intercepting authority, access to interception-related documents depended entirely on the intercepting authorities' discretion.

212. A refusal to grant access to the collected data could be appealed against to a court and the OSAA required the intercepting authorities to produce, at the judge's request, 'operational-search materials containing information about the data to which access [had been] refused'. It was significant that the intercepting authorities were required to

submit 'information about the data' rather than the data themselves. Materials containing information about undercover agents or police informers could not be submitted to the court and were thereby excluded from the scope of judicial review.

(β) The Government

213. The Government submitted that under Russian law, an individual subject to secret surveillance measures did not have to be informed of those measures at any point. The Constitutional Court held (…) that in view of the necessity to keep the surveillance measures secret, the principles of a public hearing and adversarial proceedings were not applicable to the interception authorisation proceedings. The person concerned was therefore not entitled to participate in the authorisation proceedings or to be informed about the decision taken.

214. After the termination of the investigation the defendant was entitled to study all the materials in the criminal case-file, including the data obtained in the course of operational-search activities. Otherwise, in cases where the investigator decided not to open criminal proceedings against the interception subject or to discontinue the criminal proceedings on the ground that the alleged offence had not been committed or one or more elements of a criminal offence were missing, the interception subject was entitled to request and receive information about the data collected. A refusal to provide such information could be challenged before a court, which had power to order the disclosure of information if it considered the refusal to be ill-founded. The Government submitted a copy of the decision of 4 August 2009 by the Alekseyevskiy District Court of the Belgorod Region, ordering that the police provide, within one month, an interception subject with information about the data collected about him in the course of the interception 'to the extent permitted by the requirements of confidentiality and with the exception of data which could enable State secrets to be disclosed'.

215. The Government argued that Russian law was different from the Bulgarian law criticised by the Court in its judgment of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, § 91)because it provided for a possibility to declassify the interception materials and to grant the person concerned access to them. In support of that allegation they referred to the criminal conviction judgment of 11 July 2012 by the Zabaykalsk Regional Court. That judgment — a copy of which was not provided to the Court — relied, according to the Government, on a judicial decision authorising the interception of the defendant's telephone communications which had been declassified and submitted to the trial judge at his request. The Government also referred to two further judgments — by the Presidium of the Krasnoyarsk Regional Court and the Presidium of the Supreme Court of the Mariy-El Republic — quashing by way of supervisory review judicial decisions authorising interception of communications. They did not submit copies of the judgments.

(viii) Available remedies

(α) The applicant

216. The applicant submitted that the questions of notification of surveillance measures and of the effectiveness of remedies before the courts were inextricably linked, since there was in principle little scope for recourse to the courts by the individual concerned unless the latter was advised of the measures taken without his or her knowledge and was thus able to challenge their legality retrospectively (he referred to *Weber and Saravia*, cited above).

217. The applicant argued that remedies available under Russian law were ineffective. As regards the possibility for the subject of surveillance to apply for judicial review of the measures applied, the burden of proof was on the claimant to demonstrate that his or her telephone had been tapped. However, since those monitored were not informed about the surveillance measures unless charged with a criminal offence, the burden of proof was impossible to satisfy. The copies of domestic judgments submitted by the Government concerned searches and seizures, that is, operative-search measures which were known to the person concerned (see paragraphs 220, 221 and 223 below). The applicant knew of no publicly available judicial decisions where an interception subject's complaint about unlawful interception had been allowed. It was also significant that in none of the judgments produced by the Government had the domestic courts assessed the proportionality of the contested operative-search measures. The domestic proceedings brought by the applicant had also clearly demonstrated that remedies available under Russian law were ineffective. Moreover, in the case of *Avanesyan v. Russia* (no. 41152/06, 18 September 2014) the Court had already found that there were no effective remedies under Russian law to challenge operational-search measures.

218. Lastly, the applicant submitted that an interception subject or the communications service providers could not challenge the ministerial orders governing secret interceptions of communications, because those orders were considered to be technical rather than legal in nature and were therefore not subject to judicial review, as demonstrated by the decisions mentioned in paragraph 161 above.

(β) The Government

219. The Government argued that in Russia a person claiming that his or her rights had been or were being violated by a State official performing operational-search activities was entitled to complain to the official's superior, the prosecutor or a court, in accordance with section 5 of the OSAA (…).

220. As explained by the Plenary Supreme Court, if the person concerned learned about the interception, he or she could apply to a court of ge-

neral jurisdiction in accordance with the procedure established by Chapter 25 of the Code of Civil Procedure (…). According to the Government, a claimant did not have to prove that his or her right had been breached as a result of the interception measures. The burden of proof was on the intercepting authorities to show that the interception measures had been lawful and justified. Russian law provided that if a breach of the claimant's rights was found by a court in civil proceedings, the court had to take measures to remedy the violation and compensate the damage (…). The Government submitted copies of two judicial decisions under Chapter 25 of the Code of Civil Procedure, declaring searches and seizures of objects or documents unlawful and ordering the police to take specific measures to remedy the violations.

221. Furthermore, according to the Government, the interception subject was also entitled to lodge a supervisory-review complaint against the judicial decision authorising the interception, as explained by the Constitutional Court in its decision of 15 July 2008 (…). He or she was likewise entitled to lodge an appeal or a cassation appeal.

222. If the interception was carried out in the framework of criminal proceedings, the person concerned could also lodge a complaint under Article 125 of the CCrP. The Government referred to the Supreme Court's decision of 26 October 2010 quashing, by way of supervisory review, the lower courts' decisions to declare inadmissible K.'s complaint under Article 125 of the CCrP about the investigator's refusal to give her a copy of the judicial decision authorising interception of her communications. The Supreme Court held that her complaint was to be examined under Article 125 of the CCrP, despite the fact that she had been already convicted, and that she was entitled to receive a copy of the interception authorisation. The Government submitted copies of ten judicial decisions allowing complaints under Article 125 of the CCrP about unlawful searches and seizures of objects or documents. They also produced a copy of a judgment acquitting a defendant on appeal after finding that his conviction at first instance had been based on inadmissible evidence obtained as a result of an unlawful test purchase of drugs.

223. The Government further submitted that the person concerned could apply for compensation under Article 1069 of the Civil Code (…). That Article provided for compensation of pecuniary and non-pecuniary damage caused to an individual or a legal entity by unlawful actions by State and municipal bodies and officials, provided that the body's or the official's fault had been established. Compensation for non-pecuniary damage was determined in accordance with the rules set out in Articles 1099-1101 of the Civil Code (…). The Government highlighted, in particular, that non-pecuniary damage caused through dissemination of information which was damaging to honour, dignity or reputation could be compensated irrespective of the tortfeasor's fault. The Government submitted a copy of a decision of 9 December 2013 by the Vichuga Town Court of the Ivanovo Region, awarding compensation in respect of non-pecuniary damage for unlawful interception of a suspect's telephone conversations after the recordings obtained as a result of that interception had been declared inadmissible as evidence by the trial court. The Government also submitted a judicial decision awarding compensation for an unlawful search and seizure of documents and a judicial decision awarding compensation to an acquitted defendant for unlawful prosecution.

224. Russian law also provided for criminal remedies for abuse of power (Articles 285 and 286 of the Criminal Code), unauthorised collection or dissemination of information about a person's private and family life (Article 137 of the Criminal Code) and breach of citizens' right to privacy of communications (Article 138 of the Criminal Code) (…). The Government referred in that connection to the Supreme Court's judgment of 24 October 2002, convicting a certain E.S. of an offence under Article 138 of the Criminal Code for inciting an official to supply him with the names of the owners of several telephone numbers and to provide him with call detail records in respect of those telephone numbers. They also referred to the Supreme Court's judgment of 15 March 2007, convicting a customs official of an offence under Article 138 of the Criminal Code for intercepting the telephone communications of a certain P. They submitted copies of two more conviction judgments under Article 138 of the Criminal Code: the first conviction concerned the selling of espionage equipment, namely pens and watches with in-build cameras, while the second conviction concerned the covert hacking of a communication provider's database in order to obtain the users' call detail records.

225. Lastly, the Government argued that remedies were also available in Russian law to challenge the alleged insufficiency of safeguards against abuse in the sphere of interception of communications (see paragraph 156 above).

226. The Government submitted that the applicant had not used any of the remedies available to him under Russian law and described above. In particular, he had chosen to bring judicial proceedings against mobile network operators, the Ministry of Communications being joined only as a third party to the proceedings.

(b) The Court's assessment

(i) General principles

227. The Court reiterates that any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim (see *Kennedy*, cited above, § 130).

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 [*NJ* 2009/410, m.nt. E.A. Alkema; *red.*], § 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 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).

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

235. The Court notes that it has found there to be an interference under Article 8 § 1 in respect of the applicant's general complaint about Russian legislation governing covert interception of mobile telephone communications. Accordingly, in its examination of the justification for the interference under Article 8 § 2, the Court is required to examine whether the contested legislation itself is in conformity with the Convention.

236. In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the 'necessity' test has been complied with and it is therefore appropriate for the Court to address jointly the 'in accordance with the law' and 'necessity' requirements (see *Kennedy*, cited above, § 155; see also *Kvasnica*, cited above, § 84). The 'quality of law' in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when 'necessary in a democratic society', in particular by providing for adequate and effective safeguards and guarantees against abuse.

237. It has not been disputed by the parties that interceptions of mobile telephone communications have a basis in the domestic law. They are governed, in particular, by the CCrP and the OSAA, as well as by the Communications Act and the Orders issued by the Ministry of Communications. Furthermore, the Court considers it clear that the surveillance measures permitted by Russian law pursue the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country (…). It therefore remains to be ascertained whether the domestic law is accessible and contains adequate and effective safeguards and guarantees to meet the requirements of 'foreseeability' and 'necessity in a democratic society'.

238. The Court will therefore assess in turn the accessibility of the domestic law, the scope and duration of the secret surveillance measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.

(α) Accessibility of domestic law

239. It is common ground between the parties that almost all legal provisions governing secret surveillance — including the CCrP, the OSAA, the Communications Act and the majority of the Orders issued by the Ministry of Communications — have been officially published and are accessible to the public. The parties disputed, however, whether the addendums to Order no. 70 by the Ministry of Communications met the requirements of accessibility.

240. The Court observes that the addendums to Order no. 70 have never been published in a generally accessible official publication, as they were considered to be technical in nature (…).

241. The Court accepts that the addendums to Order no. 70 mainly describe the technical requirements for the interception equipment to be installed by communications service providers. At the same time, by requiring that the equipment at issue must ensure that the law-enforcement authorities have direct access to all mobile telephone communications of all users and must not log or record information about interceptions initiated by the law-enforcement authorities (…), the addendums to Order No. 70 are capable of affecting the users' right to respect for their private life and correspondence. The Court therefore considers that they must be accessible to the public.

242. The publication of the Order in the Ministry of Communications' official magazine *SvyazInform*, distributed through subscription, made it available only to communications specialists rather than to the public at large. At the same time, the Court notes that the text of the Order, with the addendums, can be accessed through a privately-maintained internet legal database, which reproduced it from the publication in *SvyazInform* (…). The Court finds the lack of a generally accessible official publication of Order no. 70 regrettable. However, taking into account the fact that it has been published in an official ministerial magazine, combined with the fact that it can be accessed by the general public through an internet legal database, the Court does not find it

necessary to pursue further the issue of the accessibility of domestic law. It will concentrate instead on the requirements of 'foreseeability' and 'necessity'.

(β) Scope of application of secret surveillance measures

243. The Court reiterates that the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures — in particular by clearly setting out the nature of the offences which may give rise to an interception order and a definition of the categories of people liable to have their telephones tapped (see paragraph 231 above).

244. As regards the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively, by name, the specific offences which may give rise to interception. However, sufficient detail should be provided on the nature of the offences in question (see *Kennedy*, cited above, § 159). Both the OSAA and the CCrP provide that telephone and other communications may be intercepted in connection with an offence of medium severity, a serious offence or an especially serious criminal offence — that is, an offence for which the Criminal Code prescribes a maximum penalty of more than three years' imprisonment — which has been already committed, is ongoing or being plotted (…). The Court considers that the nature of the offences which may give rise to an interception order is sufficiently clear. At the same time it notes with concern that Russian law allows secret interception of communications in respect of a very wide range of criminal offences, including for example, as pointed out by the applicant, pickpocketing (see paragraph 182 above; see also, for similar reasoning, *Iordachi and Others*, cited above, §§ 43 and 44).

245. The Court further notes that interceptions may be ordered not only in respect of a suspect or an accused, but also in respect of a person who may have information about an offence or may have other information relevant to the criminal case (…). The Court has earlier found that interception measures in respect of a person who was not suspected of any offence but could possess information about such an offence might be justified under Article 8 of the Convention (see *Greuter*, cited above). At the same time, the Court notes the absence of any clarifications in Russian legislation or established case-law as to how the terms 'a person who may have information about a criminal offence' and 'a person who may have information relevant to the criminal case' are to be applied in practice (see, for similar reasoning, *Iordachi and Others*, cited above, § 44).

246. The Court also observes that in addition to interceptions for the purposes of preventing or detecting criminal offences, the OSAA also provides that telephone or other communications may be intercepted following the receipt of information about events or activities endangering Russia's national, military, economic or ecological security (…). Which events or activities may be considered as endangering such types of security interests is nowhere defined in Russian law.

247. The Court has previously found that the requirement of 'foreseeability' of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on 'national security' grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance (see *Kennedy*, cited above, § 159). At the same time, the Court has also emphasised that in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of 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, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see *Liu v. Russia*, no. 42086/05, § 56, 6 December 2007, with further references).

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.

(γ) The duration of secret surveillance measures

250. The Court has held that it is not unreasonable to leave the overall duration of interception to the discretion of the relevant domestic autho-

rities which have competence to issue and renew interception warrants, provided that adequate safeguards exist, such as a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled (see *Kennedy*, cited above, § 161; see also *Klass and Others*, cited above, 52, and *Weber and Saravia*, cited above, § 98).

251. As regards the first safeguard, both the CCrP and the OSAA provide that interceptions may be authorised by a judge for a period not exceeding six months (…). There is therefore a clear indication in the domestic law of the period after which an interception authorisation will expire. Secondly, the conditions under which an authorisation can be renewed are also clearly set out in law. In particular, under both the CCrP and the OSAA a judge may extend interception for a maximum of six months at a time, after a fresh examination of all the relevant materials (id.). However, as regards the third safeguard concerning the circumstances in which the interception must be discontinued, the Court notes that the requirement to discontinue interception when no longer necessary is mentioned in the CCrP only. Regrettably, the OSAA does not contain such a requirement (id.). In practice, this means that interceptions in the framework of criminal proceedings are attended by more safeguards than interceptions conducted outside such a framework, in particular in connection with 'events or activities endangering national, military, economic or ecological security'.

252. The Court concludes from the above that while Russian law contains clear rules on the duration and renewal of interceptions providing adequate safeguards against abuse, the OSAA provisions on discontinuation of the surveillance measures do not provide sufficient guarantees against arbitrary interference.

(δ) Procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data

253. Russian law stipulates that data collected as a result of secret surveillance measures constitute a State secret and are to be sealed and stored under conditions excluding any risk of unauthorised access. They may be disclosed to those State officials who genuinely need the data for the performance of their duties and have the appropriate level of security clearance. Steps must be taken to ensure that only the amount of information needed by the recipient to perform his or her duties is disclosed, and no more. The official responsible for ensuring that the data are securely stored and inaccessible to those without the necessary security clearance is clearly defined (…). Domestic law also sets out the conditions and procedures for communicating intercepted data containing information about a criminal offence to the prosecuting authorities. It describes, in particular, the requirements for their secure storage and the conditions for their use as evidence in criminal proceedings (…). The Court is satisfied that Russian law contains clear rules governing the storage, use and communication of intercepted data, making it possible to minimise the risk of unauthorised access or disclosure (see, for similar reasoning, *Kennedy*, cited above, §§ 62 and 63).

254. As far as the destruction of intercept material is concerned, domestic law provides that intercept material must be destroyed after six months of storage, if the person concerned has not been charged with a criminal offence. If the person has been charged with a criminal offence, the trial judge must make a decision, at the end of the criminal proceedings, on the further storage and destruction of the intercept material used in evidence (…).

255. As regards the cases where the person concerned has not been charged with a criminal offence, the Court is not convinced by the applicant's argument that Russian law permits storage of the intercept material beyond the statutory time-limit (see paragraph 188 above). It appears that the provision referred to by the applicant does not apply to the specific case of storage of data collected as a result of interception of communications. The Court considers the six-month storage time-limit set out in Russian law for such data reasonable. At the same time, it deplores the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they has been obtained (compare *Klass and Others*, cited above, § 52, and *Kennedy*, cited above, § 162). The automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8.

256. Furthermore, as regards the cases where the person has been charged with a criminal offence, the Court notes with concern that Russian law allows unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial (…). Russian law does not give citizens any indication as to the circumstances in which the intercept material may be stored after the end of the trial. The Court therefore considers that the domestic law is not sufficiently clear on this point.

(ε) Authorisation of interceptions

Authorisation procedures

257. The Court will take into account a number of factors in assessing whether the authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration. These factors include, in particular, the authority competent to authorise the surveillance, its scope of review and the content of the interception authorisation.

258. As regards the authority competent to authorise the surveillance, authorising of telephone tapping by a non-judicial authority may be compatible with the Convention (see, for example, *Klass and Others*, cited above, § 51; *Weber and Saravia*, cited above, § 115; and *Kennedy*, cited above, § 31), provided that that authority is sufficiently indepen-

dent from the executive (see *Dumitru Popescu v. Romania (no. 2)*, no. 71525/01, § 71, 26 April 2007).
259. Russian law contains an important safeguard against arbitrary or indiscriminate secret surveillance. It dictates that any interception of telephone or other communications must be authorised by a court (…). The law-enforcement agency seeking authorisation for interception must submit a reasoned request to that effect to a judge, who may require the agency to produce supporting materials (…). The judge must give reasons for the decision to authorise interceptions (…).
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 (…). 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).
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 (…). 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 (…). 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 (…). 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.

266. The Court further notes that in cases of urgency it is possible to intercept communications without prior judicial authorisation for up to forty-eight hours. A judge must be informed of any such case within twenty-four hours from the commencement of the interception. If no judicial authorisation has been issued within forty-eight hours, the interception must be stopped immediately (…). The Court has already examined the 'urgency' procedure provided for in Bulgarian law and found that it was compatible with the Convention (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, §§ 16 and 82). However, in contrast to the Bulgarian provision, the Russian 'urgent procedure' does not provide for sufficient safeguards to ensure that it is used sparingly and only in duly justified cases. Thus, although in the criminal sphere the OSAA limits recourse to the urgency procedure to cases where there exists an immediate danger that a serious or especially serious offence may be committed, it does not contain any such limitations in respect of secret surveillance in connection with events or activities endangering national, military, economic or ecological security. The domestic law does not limit the use of the urgency procedure to cases involving an immediate serious danger to national, military, economic or ecological security. It leaves the authorities an unlimited degree of discretion in determining in which situations it is justified to use the non-judicial urgent procedure, thereby creating possibilities for abusive recourse to it (see, by contrast, *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 16). Furthermore, although Russian law requires that a judge be immediately informed of each instance of urgent interception, his or her power is limited to authorising the extension of the interception measure beyond forty-eight hours. He or she has no power to assess whether the use of the urgent procedure was justified or to decide whether the material obtained during the previous forty-eight hours is to be kept or destroyed (see, by contrast, *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 16). Russian law does therefore not provide for an effective judicial review of the urgency procedure.

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.

The authorities' access to communications

268. The Court takes note of the applicant's argument that the security services and the police have the technical means to intercept mobile telephone communications without obtaining judicial authorisation, as they have direct access to all communications and as their ability to intercept the communications of a particular individual or individuals is not conditional on providing an interception authorisation to the communications service provider.

269. The Court considers that the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception. In Russia the law-enforcement authorities are not required under domestic law to show the judicial authorisation to the communications service provider before obtaining access to a person's communications (see, by contrast, the EU Council Resolution cited in paragraph 145 above), except in connection with the monitoring of communications-related data under the CCrP (…). Indeed, pursuant to Orders issued by the Ministry of Communications, in particular the addendums to Order No. 70, communications service providers must install equipment giving the law-enforcement authorities direct access to all mobile telephone communications of all users (…). The communications service providers also have an obligation under Order no. 538 to create databases storing information about all subscribers, and the services provided to them, for three years; the secret services have direct remote access to those databases (…). The law-enforcement authorities thus have direct access to all mobile telephone communications and related communications data.

270. The Court considers that the manner in which the system of secret surveillance operates in Russia gives the security services and the police technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation. Alt-

hough the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system (see *Klass and Others*, cited above, § 59), the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great.

271. The Court will therefore examine with particular attention whether the supervision arrangements provided by Russian law are capable of ensuring that all interceptions are performed lawfully on the basis of proper judicial authorisation.

(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 (…). 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.

273. As regards supervision of interceptions carried out on the basis of proper judicial authorisations, the Court will examine whether the supervision arrangements existing in Russia are capable of ensuring that the statutory requirements relating to the implementation of the surveillance measures, the storage, access to, use, processing, communication and destruction of intercept material are routinely respected.

274. A court which has granted authorisation for interception has no competence to supervise its implementation. It is not informed of the results of the interceptions and has no power to review whether the requirements of the decision granting authorisation were complied with. Nor do Russian courts in general have competence to carry out the overall supervision of interceptions. Judicial supervision is limited to the initial authorisation stage. Subsequent supervision is entrusted to the President, Parliament, the Government, the Prosecutor General and competent lower-level prosecutors.

275. The Court has earlier found that, although it is in principle desirable to entrust supervisory control to a judge, supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control (see *Klass and Others*, cited above, § 56).

276. As far as the President, Parliament and the Government are concerned, Russian law does not set out the manner in which they may supervise interceptions. There are no publicly available regulations or instructions describing the scope of their review, the conditions under which it may be carried out, the procedures for reviewing the surveillance measures or for remedying the breaches detected (see, for similar reasoning, *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 88).

277. As regards supervision of interceptions by prosecutors, the Court observes that the national law sets out the scope of, and the procedures for, prosecutors' supervision of operational-search activities (…). It stipulates that prosecutors may carry out routine and *ad hoc* inspections of agencies performing operational-search activities and are entitled to study the relevant documents, including confidential ones. They may take measures to stop or remedy the detected breaches of law and to bring those responsible to liability. They must submit semi-annual reports detailing the results of the inspections to the Prosecutor General's Office. The Court accepts that a legal framework exists which provides, at least in theory, for some supervision by prosecutors of secret surveillance measures. It must be next examined whether the prosecutors are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise effective and continuous control.

278. As to the independence requirement, in previous cases the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it found sufficiently independent the bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by parliament or by the Prime Minister (see, for example, *Klass and Others*, cited above, §§ 21 and 56; *Weber and Saravia*, cited above, §§ 24, 25 and 117; *Leander*, cited above, § 65; (see *L. v. Norway*, no. 13564/88, Commission decision of 8 June 1990); and *Kennedy*, cited above, §§ 57 and 166). In contrast, a Minister of Internal Affairs — who not only was a political appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance — was found to be insufficiently independent (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, §§ 85 and 87). Similarly, a Prosecutor General and competent lower-level prosecutors were also found to be insuf-

ficiently independent (see *Iordachi and Others*, cited above, § 47).
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 (…). 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 prosecutor's offices do not specialise in supervision of interceptions (…). 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 (…). This blending of functions within one prosecutor's 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 (…). 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 (…). As individuals are not notified of interceptions (see … 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 (…). However, there is no specific provision requiring destruction of the unlawfully obtained intercept material (see *Kennedy*, cited above, § 168).
283. The Court must also examine whether the supervisory body's activities are open to public scrutiny (see, for example, *L. v. Norway*, cited above, where the supervision was performed by the Control Committee, which reported annually to the Government and whose reports were published and discussed by Parliament; *Kennedy*, cited above, § 166, where the supervision of interceptions was performed by the Interception of Communications Commissioner, who reported annually to the Prime Minister, his report being a public document laid before Parliament; and, by contrast, *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 88, where the Court found fault with the system where neither the Minister of Internal Affairs nor any other official was required to report regularly to an independent body or to the general public on the overall operation of the system or on the measures applied in individual cases). In Russia, prosecutors must submit semi-annual reports detailing the results of the inspections to the Prosecutor General's Office. However, these reports concern all types of operational-search measures, amalgamated together, without interceptions being treated separately from other measures. Moreover, the reports contain only statistical information about the number of inspections of operational-search measures carried out and the number of breaches detected, without specifying the nature of the breaches or the measures taken to remedy them. It is also significant that the reports are confidential documents. They are not published or otherwise accessible to the public (…). It follows that in Russia supervision by prosecutors is conducted in a manner which is not open to public scrutiny and knowledge.
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 (…). 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

286. The Court will now turn to the issue of notification of interception of communications which is inextricably linked to the effectiveness of remedies before the courts (see case-law cited in paragraph 234 above).

287. It may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not 'necessary in a democratic society', as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned (see *Klass and Others*, cited above, § 58, and *Weber and Saravia*, cited above, § 135). The Court also takes note of the Recommendation of the Committee of Ministers regulating the use of personal data in the police sector, which provides that where data concerning an individual have been collected and stored without his or her knowledge, and unless the data are deleted, he or she should be informed, where practicable, that information is held about him or her as soon as the object of the police activities is no longer likely to be prejudiced (§ 2.2 …).

288. In the cases of *Klass and Others* and *Weber and Saravia* the Court examined German legislation which provided for notification of surveillance as soon as that could be done after its termination without jeopardising its purpose. The Court took into account that it was an independent authority, the G10 Commission, which had the power to decide whether an individual being monitored was to be notified of a surveillance measure. The Court found that the provision in question ensured an effective notification mechanism which contributed to keeping the interference with the secrecy of telecommunications within the limits of what was necessary to achieve the legitimate aims pursued (see *Klass and Others*, cited above, § 58, and *Weber and Saravia*, cited above, § 136). In the cases of *Association for European Integration and Human Rights and Ekimdzhiev* and *Dumitru Popescu (no. 2)*, the Court found that the absence of a requirement to notify the subject of interception at any point was incompatible with the Convention, in that it deprived the interception subject of an opportunity to seek redress for unlawful interferences with his or her Article 8 rights and rendered the remedies available under the national law theoretical and illusory rather than practical and effective. The national law thus eschewed an important safeguard against the improper use of special means of surveillance (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, §§ 90 and 91, and *Dumitru Popescu (no. 2)*, cited above, § 77). By contrast, in the case of *Kennedy* the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications (see *Kennedy*, cited above, § 167).

289. Turning now to the circumstances of the present case, the Court observes that in Russia persons whose communications have been intercepted are not notified of this fact at any point or under any circumstances. It follows that, unless criminal proceedings have been opened against the interception subject and the intercepted data have been used in evidence, or unless there has been a leak, the person concerned is unlikely ever to find out if his or her communications have been intercepted.

290. The Court takes note of the fact that a person who has somehow learned that his or her communications have been intercepted may request information about the corresponding data (…). It is worth noting in this connection that in order to be entitled to lodge such a request the person must be in possession of the facts of the operational-search measures to which he or she was subjected. It follows that the access to information is conditional on the person's ability to prove that his or her communications were intercepted. Furthermore, the interception subject is not entitled to obtain access to documents relating to interception of his or her communications; he or she is at best entitled to receive 'information' about the collected data. Such information is provided only in very limited circumstances, namely if the person's guilt has not been proved in accordance with the procedure prescribed by law, that is, he or she has not been charged or the charges have been dropped on the ground that the alleged offence was not committed or that one

or more elements of a criminal offence were missing. It is also significant that only information that does not contain State secrets may be disclosed to the interception subject and that under Russian law information about the facilities used in operational-search activities, the methods employed, the officials involved and the data collected constitutes a State secret (…). In view of the above features of Russian law, the possibility to obtain information about interceptions appears to be ineffective.

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 (…). 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 [*NJ* 2002/180, m.nt. T.M. Schalken], §§ 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 … *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 (…). 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.

295. Further, a complaint under Article 125 of the CCrP may be lodged only by a participant to criminal proceedings while a pre-trial investigation is pending (…). This remedy is therefore available only to persons who have learned about the interception of their communications in the framework of criminal proceedings against them. It cannot be used by a person against whom no criminal proceedings have been brought following the interception of his or her communications and who does not know whether his or her communications were intercepted. It is also worth noting that the Government did not submit any judicial decisions examining a complaint under Article 125 of the CCrP about the interception of communications. They therefore failed to illustrate the practical effectiveness of the remedy invoked by them with examples from the case-law of the domestic courts (see, for similar reasoning, *Rotaru*, cited above, § 70, and *Ananyev and Others*, cited above, §§ 109 and 110).

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 (…). 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 (…). 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 (…).

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. It is not the Court's task in the present case to decide whether these remedies will be effective in cases where an individual learns about the interception of his or her communications in the course of criminal proceedings against him or her (see, however, *Avanesyan*, cited above, where some of these remedies were found to be ineffective to complain about an 'inspection' of the applicant's flat).

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 (…). 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 (…). It is also significant that the Supreme Court found that Order no. 70 was technical rather than legal in nature (…).

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 (…) 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.

II. Alleged violation of Article 13 of the Convention

306. The applicant complained that he had no effective remedy for his complaint under Article 8. He relied on Article 13 of the Convention, which reads as follows:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

307. Having regard to the findings under Article 8 of the Convention in paragraphs 286 to 300 above, the Court considers that, although the complaint under Article 13 of the Convention is closely linked to the complaint under Article 8 and therefore has to be declared admissible, it is not necessary to examine it separately (see *Liberty and Others*, cited above, § 73).

III. Application of Article 41 of the Convention

Enz. (*Red.*)

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, € 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.

Concurring opinion of Judge Dedov

1. Competence of the Court to examine the domestic law in abstracto

As pointed out by the Government, doubts may exist as to the Court's competence to examine the quality and effectiveness of the domestic law *in abstracto* without the applicant's victim status being established and without determining that there had been interference with his right to respect for his private life in practice, and not merely theoretically.

This approach has already been used by the Court in interception cases in order to prevent potential abuses of power. In two leading cases, *Kennedy v. the United Kingdom* (no. 26839/05, §§ 122-123, 18 May 2010) and *Klass and Others v. Germany* (6 September 1978, § 34, Series A no. 28), against two prominent democratic States, namely the United Kingdom and the Federal Republic of Germany, the Court confirmed the effectiveness of the relevant domestic systems against arbitrariness. However, and regrettably, we cannot ignore the fact that both of these States have recently been involved in major well-publicised surveillance scandals. Firstly, the mobile telephone conversations of the Federal Chancellor of Germany were unlawfully intercepted by the national secret service; and secondly, the UK authorities provided a US secret service with access to and information about the former State's entire communication database, with the result that the US authorities were able to intercept all UK citizens without being subject to any appropriate domestic safeguards at all.

This indicates that something was wrong with the Court's approach from the very outset. It would perhaps be more effective to deal with applications on an individual basis, so that the Court has an opportunity to establish interference and to find a violation of the Convention, as indeed it regularly finds in relation to unjustified searches of applicants' premises. Generally speaking, the problem in those cases does not concern the authorisation powers of the domestic courts, but the manner in which the judges authorise the requests for investigative searches.

The Court's approach can easily shift from the actual application of the law to the potential for interference. Here are examples from the Kennedy case:

> "119. The Court has consistently held in its case-law that its task is not normally to review the relevant law and practice *in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention (see, *inter alia, Klass and Others*, cited above, § 33; *N.C. v. Italy [GC]*, no. 24952/94, § 56, ECHR 2002-X; and *Krone Verlag GmbH & Co. KG v. Austria (no. 4)*, no. 72331/01, § 26, 9 November 2006)";

and from the *Klass* case:

> "36 …The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25 …, since otherwise Article 8 … runs the risk of being nullified".

However, the German and English scandals referred to above confirm that, sooner or later, the individual concerned will become aware of the interception. One may find relevant examples in the Russian context (see *Shimovolos v. Russia*, no. 30194/09, 21 June 2011). The applicant in the present case is not aware of any interception of his communications, and this fact cannot be ignored by the Court.

The Court has on many occasions avoided examining cases *in abstracto* (see *Silver and Others v. the United Kingdom*, 25 March 1983, Series A no. 61, § 79; *Nikolova v. Bulgaria [GC]*, no. 31195/96, § 60, ECHR 1999-II; *Nejdet Şahin and Perihan Şahin v. Turkey* [GC], no. 13279/05, §§ 68-70, 20 October 2011; *Sabanchiyeva and Others v. Russia*, no. 38450/05, § 137, ECHR 2013; and *Monnat v. Switzerland*, no. 73604/01, §§ 31-32, ECHR 2006-X). Thus, one can presume that the interception cases are unique. We then need to know the reasons why the Court should change its general approach when examining such cases. Yet we have no idea about what those reasons might be. If the legislation creates the risk of arbitrariness, then we need to see the outcome of that arbitrariness. I am not sure that a few examples (unrelated to the applicant's case) prove that the entire system of safeguards should be revised and strengthened. I would accept such an approach if the Court had a huge backlog of individual repetitive petitions showing that Order no. 70 (on the connection of interception equipment to operators' networks) is not technical in nature but that it creates a structural problem in Russia. If that is the case, however, we need a pilot procedure and a pilot judgment.

Every case in which the Court has found a violation of the Convention (more than 15,000 judgments) is based on the abuse of power, even where the domestic legislation is of good quality. Every abuse of power is a question of ethics, and cannot be eliminated by legislative measures alone.

The Court has consistently held that its task is not to review domestic law and practice *in abstracto* or to express a view as to the compatibility of the provisions of legislation with the Convention, but to determine whether the manner in which they were applied or in which they affected the applicant gave rise to a violation of the Convention (see, among other authorities, in the Article 14 context, *Religionsgemeinschaft der Zeugen Jehovas and Others v. Austria*, no. 40825/98, § 90, 31 July 2008).

Article 34 of the Convention does not institute for individuals a kind of *actio popularis* for the interpretation of the Convention; it does not permit individuals to complain against a law *in abstracto* simply because they feel that it contravenes the Convention. In principle, it does not suffice for an individual applicant to claim that the mere existence of a law violates his rights under the Convention; it is necessary that the law should have been applied to his detriment (see *Klass*, cited above, § 33). These principles should not be applied arbitrarily.

2. Legislature and judiciary: the Court should respect differences

This case is very important in terms of the separation of functions between the Court and the Parliamentary Assembly of the Council of Europe, as it is necessary to separate the powers of the legislature and judiciary. The Parliamentary Assembly adopts recommendations, resolutions and opinions which serve as guidelines for the Committee of Ministers, national governments, parliaments and political parties. Ultimately, through conventions, legislation and practice, the Council of Europe promotes human rights, democracy and the rule of law. It monitors member States' progress in these areas and makes recommendations through independent expert monitoring bodies. The European Court of Human Rights rules on individual or State applications alleging violations of the civil and political rights set out in the European Convention on Human Rights. Taking account of the above separation of functions, the examination of a case *in abstracto* is similar to an expert report, but not to a judgment.

Morten Kjaerum, Director of European Union Agency for Human Rights (FRA), addressed a joint debate on fundamental rights at the European Parliamentary Committee on Civil Liberties, Justice and Home Affairs (LIBE) on 4 September 2014. The Director pointed out:

> "The Snowden revelations of mass surveillance highlighted the fact that the protection of personal data is under threat. The protection of the right to privacy is far from sufficient when we look across Europe today. Following last year's debates, we very much welcome the European Parliament's request to the Fundamental Rights Agency to further investigate the fundamental rights and safeguards in place in the context of large-scale surveillance programmes. And of course you will be informed probably towards the end of this year about the findings of this particular request.
>
> But it's not only the big surveillance programmes. There are also misgivings about oversight mechanisms in the area of general data protection. When we give data to health authorities, to tax authorities, to other institutions, public or private. We see from the work of the Fundamental Rights Agency that the national oversight structures in the EU are currently too weak to fulfil their mission. Data protection authorities, which are established in all Member States have an important role to play in the enforcement of

the overall data protection system, but the powers and resources of national data protection authorities urgently needs to be strengthened and also their independence needs to be guaranteed.

Finally, I would also highlight that those who are entrusted to store the data, whether it is private or public, that the institutions need to be accountable, at a much stronger level that we see today if the safeguards that they create are not sufficiently in place."

These remarks were addressed to the newly elected members of the European Parliament (rather than to judges), raising issues of concern across Europe and calling for more a sophisticated system of data protection. The aim of the speech was to initiate public debate in order to find effective measures and to promote proper ethical standards in society; the courtroom is not a place for such a debate.

I would suggest that the Court more properly focus on a particular interference and the effectiveness of the measures in place to prevent that specific violation (as the Court usually does in all other categories of cases). This is the Court's primary task: to establish that an interference has taken place and then to examine whether the interference was lawful and necessary in a democratic society. It is ethically unacceptable for judges to presume that every citizen in a particular country could be under unlawful secret surveillance without knowledge of the facts. A judgment cannot be built on the basis of allegations.

The Court has used many tools to fight against violations. One of them was to find a violation of Article 10 on account of an intelligence service's refusal to provide information to the applicant organisation about individuals placed under electronic surveillance for a specified period (*Youth Initiative for Human Rights v. Serbia*, no. 48135/06, 25 June 2013). In the operative part of that judgment, the Court invited the Government to ensure that the disputed information was made available to the applicant organisation (without waiting for measures to be proposed by the Committee of Ministers). I recognize this as an effective measure and a judicial success.

3. The 'reasonable likelihood' approach should be developed

Establishment of the applicant's victim status is an integral part of the judicial process. Article 34 of the Convention provides that 'the Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto'. The notion of 'victim' does not imply the existence of prejudice (see *Brumărescu v. Romania* [GC], no. 28342/95, § 50, ECHR 1999-VII).

The Court has previously ruled that, while the existence of a surveillance regime might interfere with privacy, a claim that this created a violation of rights was justiciable only where there was a 'reasonable likelihood' that a person had actually been subjected to unlawful surveillance (see *Esbester v. the United Kingdom*, no. 18601/91, Commission decision of 2 April 1993; *Redgrave v. the United Kingdom*, application no. 202711/92, Commission decision of 1 September 1993; and *Matthews v. the United Kingdom*, application no. 28576/95, Commission decision of 16 October 1996). These references are to inadmissibility decisions, since all of the allegations of interception were considered manifestly ill-founded.

However, the Court changed its approach completely in the *Klass* case: "… it could not be excluded that secret surveillance measures were applied to him or that the applicant was potentially at risk of being subjected to such measures" (*Klass*, cited above, §§ 125-129). Today we see that this change in the case-law was not effective.

The term 'reasonable likelihood' implies that there are negative consequences for an applicant who is potentially subject to secret surveillance, on account of certain information that is made available to the authorities through interception, and excluding the possibility that this information could be uncovered by other means. The Court made this approach dangerously simple in order to examine the merits of these cases, presuming that persons who are subject to secret supervision by the authorities are not always subsequently informed of such measures against them, and thus it is impossible for the applicants to show that any of their rights have been interfered with. In these circumstances the Court concluded that applicants must be considered to be entitled to lodge an application even if they cannot show that they are victims. The applicants in the *Klass* and *Liberty* (*Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008) cases were lawyers and theoretically 'they could [have been] subject to secret surveillance in consequence of contacts they may have with clients who might be suspected of illegal activities' (*Klass*, § 37).

In the *Kennedy* case the applicant alleged that local calls to his telephone were not being put through to him and that he was receiving a number of time-wasting hoax calls. The applicant suspected that this was because his mail, telephone and email communications were being intercepted, and the Court took this into serious consideration, rejecting the Government's objections that the applicant had failed to show that there had been interference for the purposes of Article 8, and that he had not established a reasonable likelihood. The Court also rejected the non-exhaustion submissions, in spite of the fact that the applicant had not checked the quality of telecoms services with his operator, but had made subject access requests to MI5 and GCHQ (the United Kingdom's intelligence agencies responsible for national security) under the Data Protection Act 1998.

Returning to the circumstances of the present case, it can reasonably be concluded that the in-

terconnection between the telecoms equipment and the interception equipment does not necessary mean that interception of the applicant's telephone conversations has actually taken place. Nor can the Court base its findings on the presumption of the 'possibility of improper action by a dishonest, negligent or over-zealous official' (see *Klass*, §§ 49, 50, 59; *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 106, ECHR 2006-XI; *Kennedy*, §§ 153-154). Equally, the Court cannot presume in general (in order to examine the case *in abstracto*) the existence of State violence against the opposition movements and other democratic institutions in the respondent State, even if corresponding resolutions have been adopted by the Parliamentary Assembly. The Court must maintain its impartiality and neutrality.

4. Role of the judiciary in civil society

Nonetheless, I have voted for admissibility and for the finding of a violation of Article 8 of the Convention on account of the fact that the fundamental importance of safeguards to protect private communications against arbitrary surveillance, especially in the non-criminal context, was never addressed in the domestic proceedings. The Russian courts refused to address the applicant's allegations on the merits, mistakenly referring to the technical nature of the impugned ministerial orders. As a national judge, I cannot ignore the fact that a widespread suspicion exists in Russian society that surveillance is exercised over political and economic figures, including human-rights activists, opposition activists and leaders, journalists, State officials, managers of State property — in other words, over all those who are involved in public affairs. Such a suspicion is based on past experience of the totalitarian regime during the Soviet era, and even on the long history of the Russian Empire.

This judgment could serve as a basis for improving the legislation in the sphere of operational and search activities and for establishing an effective system of public control over surveillance. Moreover, this judgment demonstrates that if widespread suspicion exists in society, and if there is no other possibility for society to lift this suspicion without a social contract and appropriate changes in national law and practice, then where the problem is not identified by the other branches of power, the judiciary must be active in order to facilitate those changes. This is even more obvious if there are no other means available to protect democracy and the rule of law. This is an important role which the judiciary must play in civil society.

The Court could be criticised for failing to provide more specific reasoning for its *in abstracto* examination within the social context, with the observation that the Court has merely followed its own Chamber case-law. However, the judgment in the present case is a difficult one, since before reaching their conclusion the judges had to take care to establish whether or not all other means were useless. In contrast, in the case of *Clapper v. Amnesty International USA* (568 U.S. _ (2013), the US Supreme Court failed to take a step forward, despite the existence of a mass surveillance programme and 'the widespread suspicion' of its existence (or, in other words written by Justice Breyer in dissent, '[the harm] is as likely to take place as are most future events that common-sense inference and ordinary knowledge of human nature tell us will happen'). Instead, it rejected as insufficient the argument by the plaintiffs (including human-rights, legal and media organisations) that they were likely to be subject to surveillance due to the nature of their work.

I shall stop here, leaving the discussions on judicial aggression, activism or restraint for academics. I should like merely to close my opinion by quoting Edward Snowden's remark: "With each court victory, with every change in the law, we demonstrate facts are more convincing than fear. As a society, we rediscover that the value of the right is not in what it hides, but in what it protects".

Partly dissenting opinion of Judge Ziemele

1. I fully agree with the finding of a violation in this case. The Court has rendered a very important judgment on a matter of principle, since secret surveillance as carried out in the manner described in the facts of the case is, in its very essence, incompatible with the rule of law and the principles of democracy.

2. It is especially in such a context that I cannot agree with the Court's decision not to award any compensation for the non-pecuniary damage sustained. I consider that the applicant's claim for damages was very reasonable (see paragraph 309 of the judgment) and that the finding of a violation, while very important as a matter of principle in this case, is not appropriate satisfaction for the applicant's specific situation. I therefore voted against operative provision no. 4.

Noot

Het belang van het internationale toetsingskader

1. Deze uit Rusland afkomstige zaak betreft de rechtswaarborgen die het EHRM verlangt bij het inzetten van controle- en veiligheidsbevoegdheden van nationale veiligheidsdiensten. Dit is ook voor Nederland een zeer actuele kwestie: de Wet op Inlichtingen- en Veiligheidsdiensten — hierna: WIV — ondergaat substantiële wijzigingen waarbij ook de omvang van het toezicht in het Parlement uitvoerig aan de orde is (*Kamerstukken I en II* 2016/17, 34588, op het moment van het schrijven van deze noot aanhangig bij de Eerste Kamer). De Raad van State heeft in zijn advies bij dit wetsontwerp ernstige twijfel uitgesproken of het wetsontwerp, met name op het punt van het toezicht, wel in overeenstemming is met de door Straatsburg ontwikkelde criteria. Die twijfel is ook door andere adviesinstanties en de wetenschap overgenomen. Toch is het wetsvoorstel naar aanleiding van deze kritiek niet substantieel gewijzigd. Er moet dus rekening mee worden ge-

houden dat de rechter nadat de wet is aangenomen een oordeel over de verenigbaarheid van de wet met Straatsburgse normen zal moeten geven.

2. Dit is een uitspraak van de Grand Chamber waarin het Hof zijn rechtspraak over dit onderwerp consolideert en verduidelijkt. Nadien is zij in grote lijnen herhaald door een gewone kamer in de zaak *Szabó en Vissy tegen Hongarije* (EHRM 12 juni 2016, appl. 37138/14). In die zaak erkent het Hof dat er bij een terreurdreiging een noodsituatie kan zijn, waarin het minder vergaande waarborgen moet accepteren (r.o. 80 en 81 in die zaak).

3. Bij het internationale toetsingskader betrekt het Hof (r.o. 139) allereerst Resolution no. 68/167, on The Right to Privacy in the Digital Age, van 18 december 2013 van de Algemene Vergadering van de VN dat de VN-staten voorschrijft er op toe te zien dat in verband met de uitoefening van de bevoegdheden van de nationale Veiligheidsdiensten het recht van privacy wordt beschermd, en, met name: "To establish or maintain existing *independent, effective domestic oversight mechanisms* capable *of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data".* Verder pakt het Hof (r.o. 140 e.v.) naast arti. 8 EVRM, de 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981' en het aanvullende Protocol en verschillende Aanbevelingen van de Raad van Ministers (r.o. 143 en 144). Bij de EU vermeldt het Hof nadrukkelijk de uitspraken van HvJ EU over Digital Rights Ierland waarin het HvJ EU de Dataretentierichtlijn nietig verklaarde (HvJ EU 8 april 2014, zaken C-293/12 en C-594/12 samen met HvJ EU 6 oktober 2015 — zaak *Schrems/Ireland*, zaak C-362/14 — gepubliceerd met mijn noot in *NJ* 2016/446-447). In de in 2 genoemde zaak Szabó en Vissy verruimt het de scoop van het internationale recht. Het citeert daar het *Report on the Democratic oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007) (CDL-AD(2007)016-e)*. Het Hof citeert ook de aanbevelingen en conclusies uit het internationaal gezaghebbende Rapport uit 2013 van de *United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. Beide zijn ouder dan de uitspraak in de onderhavige zaak, dus niet helemaal duidelijk is waarom ze hier ontbreken. Het kan met de specifieke casus te maken hebben.

4. De onderhavige zaak gaat terug tot 2003 toen de hoofdredacteur (Zakharov) van een uitgeverij van verschillende kranten en tijdschriften zich bij de Russische rechter erover beklaagde dat zijn telefoons op grond van een niet gepubliceerd besluit van het Ministerie van Communicatie, in het arrest aangeduid als Decree nr. 70, gedurende lange tijd en op grote schaal door de Federale Veiligheidsdienst waren afgeluisterd. De klacht wordt in nationale instanties afgewezen. De Grote Kamer van het EHRM houdt de Russische wetgeving en het daarop gebaseerd Decree nr 70 tegen het licht en oordeelt unaniem dat zij op verschillende punten niet voldoen aan de strenge eisen die het Hof op grond van art. 8 EVRM in de loop der tijd heeft ontwikkeld en zoals deze voortvloeien uit de internationale rechtsregels ter zake.

Wanneer ben ik 'slachtoffer'?

5. Het probleem met klachten over (ontoereikende) wettelijke waarborgen tegen het optreden van veiligheidsdiensten is dat de maatregelen in het geheim worden genomen. Degene die door een maatregel wordt getroffen weet dus meestal niet *dat* de maatregelen zijn genomen. Dit schept een ontvankelijkheidsvraag in Straatsburg. Wie klaagt in Straatsburg moet *slachtoffer* zijn van een schending van het Verdrag (art. 35 EVRM), maar hoe weet je of je dat bent als je niet weet of te jouwen aanzien een maatregel is getroffen? Kun je tegen de gebrekkige regeling zelf klagen? Maar dat zou betekenen dat je tegen een wettelijke maatregel *in abstracto* kan klagen en dat laat het Hof over het algemeen niet toe. Het Hof geeft over dit 'slachtofferschap' in r.o. 71 een principiële beslissing. Het was al eerder met het probleem geconfronteerd in oudere zaken (o.a. de zaak *Klass* uit 1978) en recenter in de zaak *Kennedy/UK* (EHRM 18 mei 2010, appl. 26893/05), maar formuleert nu een algemene regel. Die ziet er als volgt uit: Het Hof kijkt eerst naar de reikwijdte van de wetgeving. Is die heel ruim, dan is de kans dat de klager daardoor wordt getroffen groter, hetzij omdat hij tot de groep behoort tegen wie de wetgeving zich richt of omdat zij zich richt tegen alle gebruikers van communicatieapparatuur. Ten tweede speelt een rol hoe gebrekkig het systeem van rechtsbescherming is. Is die groot dan is de kans op misbruik ook groter. Als die twee voorwaarden zijn vervuld schept dat een algemene ongerustheid onder de bevolking ('widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified'). Die algemene dreiging kan opgevat worden als een belemmering van het publiek zijn communicatiemiddelen onbevangen te gebruiken. Dan kun je dus als 'slachtoffer' worden aangemerkt. Voorziet de nationale wetgeving op het eerste gezicht wel in een redelijk systeem van rechtsmiddelen dan is de dreiging van ongelimiteerd misbruik kleiner. In dat geval rust op de klager de bewijslast van omstandigheden die de kans op misbruik jegens hem groter maken (bijvoorbeeld omdat hij tot een bepaalde groep behoort). Naarmate de wetgeving gebrekkiger is ben je dus eerder 'slachtoffer'. In dit geval (r.o. 74) leidt het Hof uit de gebrekkigheid van de wetgeving de dreiging af en vindt het een onderzoek naar de wetgeving in abstracto gerechtvaardigd. Dit laat overigens zien wat het probleem in dit soort zaken is: het Hof laat zich in dit soort zaken over het algemeen niet uit over de kwaliteit van de wetgeving zonder zich in een concreet geval te (kunnen) verdiepen (dat gebeurt in deze zaak bij uitzondering overigens wel).

De inhoud van het toezicht

6. Bij geheime afluisterzaken worden hoge eisen gesteld aan de kwaliteit van de wetgeving, of zij voldoende voorspelbaar ('foreseeable') en toegankelijk ('accessible') is (r.o. 231-234). Gelet op de technische ontwikkelingen moet de burger uit de wettelijke regels kunnen afleiden wat hij kan en mag verwachten. De wet moet volgens vaste jurisprudentie inzicht geven in: a. Bestaat er een definitie van de categorieën van personen die mogen worden afgeluisterd? b. Is de duur van het afluisteren beperkt? c. Is er een vastgelegde procedure hoe gegevens mogen worden opgeslagen, gebruikt en onderzocht? d. Liggen de voorzorgsmaatregelen vast die bij communicatie van de gegevens aan derden in acht moeten worden genomen? e. Onder welke omstandigheden mogen of moeten de gegevens worden vernietigd?

7. Het Hof stelt hoge eisen aan de inhoud van het toezicht. Ook in deze zaak is het uitgangspunt niet voor misverstand vatbaar: *"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."* Dit betekent dat het Hof een duidelijke voorkeur uitspreekt voor rechterlijke controle, en, als die vervangen wordt door een andere vorm van onafhankelijk toezicht, daarvan zal verlangen dat deze gelijkwaardige waarborgen bevat. Ik verwijs ook even naar de tekst van de door het Hof nadrukkelijk geciteerde VN resolutie (hiervoor onder 2): *'independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data'*. In de zaak *Kennedy* (EHRM 18 mei 2010, appl. 26839/05) heeft het Hof een inhoudelijke invulling gegeven welke eisen aan een andere dan een rechterlijke toezichthouder moeten worden gesteld. Dat komt vrij dicht in de buurt van een rechter. Ik citeer r.o. 167 in die zaak waar het Hof een oordeel geeft over een Engelse toezichthouder:

"*The Court recalls that it has previously indicated that 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 (see Klass and Others, cited above, § 56). In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems (see, for example, the G 10 Law discussed in the context of Klass and Others and Weber and Saravia, both cited above), any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant.*"

Overigens kan de vraag worden gesteld of die Engelse toezichthouder wel zo effectief is. Zij oordeelt in ieder geval niet ex ante. In 2015 oordeelde het IPT dat het gebruik van Prism en Upstream (aftappen van satellietverkeer) door de Britse overheid geen schending van het EVRM opleverde zie https://www.ipt-uk.com/judgments.asp?id=24. Deze zaken zijn nog aanhangig bij het EHRM.

8. Het toezicht op het gebruik van onderzoeksbevoegdheden speelt in drie stadia (r.o. 233): 1. Op het moment dat de onderzoeksbevoegdheden worden ingezet. 2. De periode dat het onderzoek wordt uitgevoerd. 3. Nadat het onderzoek is beëindigd. Het Hof aanvaardt geheimhouding in de eerste twee stadia. Omdat het individu in de stadia 1. en 2. geen rol kan spelen, moet de procedure zelf in waarborgen voorzien. In stadium 3 speelt de notificatieplicht (het geobserveerde individu wordt op de hoogte gesteld dat hij is gevolgd). Zoals het Hof in r.o. 234 uiteenzet kan notificatie aan het slachtoffer de kennis verschaffen die het hem mogelijk maakt de jegens hem getroffen maatregel aan een onafhankelijke toezichthouder (bij voorkeur dus een rechter) voor te leggen, al moet de weg naar de onafhankelijke toezichthouder ook open staan als hij vóór notificatie al een vermoeden heeft dat een maatregel jegens hem wordt uitgevoerd. In dit stadium 3. zullen dus ook de opslagaspecten (zie hiervoor onder 4 de factoren c t/m e) aan de orde komen.

Het toezicht kent in alle drie de fasen problemen die, ook als het bij een rechter is ondergebracht, het niet tot een zuivere rechterlijke procedure maakt. De zitting waar de opgelegde maatregel wordt beoordeeld is niet openbaar en in de eerste twee stadia is er geen procedure op tegenspraak in aanwezigheid van het slachtoffer. In die fasen zal de toezichthouder dus 'plaatsvervangend' moeten optreden. In de Amerikaanse procedure (het zogenaamde FISA Court) is er een advocaat die in abstracto de belangen van de potentiële slachtoffers moet behartigen (hij wordt een 'public advocate' genoemd, zie https://arstechnica.com/tech-policy/2015/11/americas-super-secret-court-names-five-lawyers-as-public-advocates/) maar ook dat is een moeilijke positie omdat deze 'abstracte advocaat' in het

geheim moet opereren. Het ontbreken van procesvertegenwoordiging in de eerste twee stadia zal ook de uitoefening van een recht van hoger beroep bemoeilijken. Dit kan alleen in stadium 2 gecompenseerd worden als het slachtoffer op basis van een vermoeden dat hij wordt gevolgd een procedure bij de toezichthouder start. Daarom is het heel belangrijk dat de rechter/toezichthouder toegang heeft tot alle geheime informatie en voldoende technische bijstand in deze steeds complexere materie van datatechnologie. Dit blijkt duidelijk uit de geciteerde overweging in de *Kennedy*-zaak, die de constante jurisprudentie van het Hof in dit opzicht bevestigt. De toezichthouder zal ook over precieze wettelijke normen moeten beschikken en hoge eisen aan de motivering van collectieve aftapbeslissingen moeten stellen. Anders dreigt een praktijk van 'stempelbeschikkingen'.

9. Uit de jurisprudentie van het Hof blijkt dat er maar een beperkte margin of appreciation is, hoewel deze varieert naar het stadium van het toezicht. De onderhavige zaak is daarvan een bevestiging. In maar liefst zestig overwegingen onderzoekt het Hof alle hiervoor genoemde aspecten van het toezicht en beoordeelt het ze bijna allemaal als te licht, niet alleen de wettelijke regels die de procedure regelen, maar ook de onderbouwing van de specifieke maatregelen zelf. Ik verwijs naar de interessante r.o. 263-267.

10. Een apart aspect van het toezicht is het politieke toezicht. Dat is weliswaar iets anders dan het (pseudo)rechterlijke toezicht, maar toch betrekt het Hof de vraag of er afdoende politiek toezicht (waaraan het ook eisen van onafhankelijkheid stelt) is bij zijn beoordeling. Dat zien we in deze zaak in r.o. 283: "The Court must also examine whether the supervisory body's activities are open to public scrutiny". In r.o. 278 had het al geconstateerd dat politiek toezicht (bijvoorbeeld door een minister) dat niet onafhankelijk is onvoldoende is. De vraag moet worden gesteld of dat niet ook geldt voor het parlementaire toezicht in Nederland in de 'Commissie Stiekem' in de Tweede Kamer waarvan de verrichtingen volkomen ondoorzichtig zijn en die niet los staat van het Parlement.

11. Ik verwijs tot slot naar Sarah Eskens, Ot van Daalen & Nico van Eijk, *Ten standards for oversight and transparency of national intelligence services,* Amsterdam: Instituut voor Informatierecht 2015 ook gepubliceerd in http://jnslp.com/2016/07/25/10-standards-oversight-transparency-national-intelligence-services/, waarin de hele jurisprudentie van het Hof wordt geanalyseerd.

EU recht

12. Het HvJ EU is door de Dataretentierichtlijn (2002/58) en het Handvest ook geconfronteerd met een soortgelijke toetsing als het EHRM waarvan het de door deze ontwikkelde jurisprudentie getrouw volgt, zonder overigens art. 8 EVRM rechtstreeks toe te passen, maar door invulling te geven aan de art. 7 en 8 van het Handvest overeenkomstig art. 52 dat het EVRM als minimum beschermingsnorm aangeeft. Tot dusver toetste het voornamelijk de kwaliteit van de EU regelingen, zie HvJ EU 8 april 2014, (*Digital Rights/Ireland*, zaken C-293/12 en C-594/12) en HvJ EU 6 oktober 2015 (zaak *Schrems/Ireland*, zaak C-362/14), *NJ* 2016/446 en NJ 2016/447, m.nt. E.J. Dommering. Dat is begrijpelijk omdat het HvJ EU op basis van prejudiciële vragen de verenigbaarheid van nationaal recht met het EU recht of van een richtlijn met het Handvest beoordeelt. De *Digital Rights* uitspraak is gevolgd door de zaak *Tele2*, HvJ EU 21 december 2016, *NJ* 2017/186. Het Hof achtte het systeem van de Dataretentierichtlijn dat de verplichting oplegt alle communicatiegegevens van telefoon en internetverkeer van alle gebruikers gedurende zekere tijd op te slaan in strijd met de art. 7 (privacy), 8 (dataprotectie) en 11 (vrijheid van meningsuiting) van het Handvest. Dat is de eerste door het EHRM geformuleerde kwaliteitseis waaraan dit soort wetgeving moet voldoen: Bestaat er een definitie van de categorieën van personen die mogen worden afgeluisterd? Het is de uitdrukking van het beginsel uit het dataprotectierecht: 'select before you collect'. Ook dit aspect zou bij een toetsing van de WIV relevant kunnen worden, omdat deze wet in de eerste fase van een onderzoek een zeer ruime verzamelbevoegdheid aan de Veiligheidsdienst toekent.

E.J. Dommering

NJ 2017/186

HOF VAN JUSTITIE VAN DE EUROPESE UNIE
21 december 2016, nr. C-203/15 en C-698/15
(K. Lenaerts, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz, J.L. da Cruz Vilaça, E. Juhász, M. Vilaras, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen, C. Lycourgos; A-G H. Saugmandsgaard Øe)
m.nt. E.J. Dommering

Art. 5, 6, 9, 15 lid 1 e-Privacyrichtlijn; art. 7, 8, 11, 52 lid 1 Handvest Grondrechten EU

RvdW 2017/251
Computerrecht 2017/50
Module Privacy en persoonsgegevens 2017/1150
ECLI:EU:C:2016:572
ECLI:EU:C:2016:970

Verzoeken om een prejudiciële beslissing, ingediend door de Kammarrätt i Stockholm (bestuursrechter in tweede aanleg Stockholm, Zweden) en de Court of Appeal (England and Wales) (Civil Division) (rechter in tweede aanleg in burgerlijke zaken, Engeland en Wales, Verenigd Koninkrijk), bij beslissingen van, respectievelijk, 29 april 2015 en 9 december 2015.

Elektronische communicatie. Verwerking van persoonsgegevens. Vertrouwelijk karakter van de