# INTRODUCTORY NOTE TO ZAKHAROV V. RUSSIA (EUR. CT. H.R.)

BY LORNA WOODS*

[December 4, 2015]
+Cite as 55 ILM 207 (2016)+

## Background

The European Court of Human Rights (ECtHR) in *Zakharov v. Russia* held that the Russian system of surveillance constituted a violation of Article 8 of the European Convention on Human Rights (ECHR).[1] This decision is not the first judgment concerning surveillance, but it is of note because it is a Grand Chamber judgment in which the ECtHR drew together strands of its existing case law. It comes at a time when national systems of surveillance are the subject of much scrutiny: further cases are pending before the ECtHR.[2]

## Facts

Roman Andreyevich Zakharov challenged the ability of the Russian security services and police to intercept communications. While Russian law envisaged the requirement of judicial authorization for interception, it also required mobile operators to install technology allowing the security forces and police direct access to the mobile networks. His challenges before the national courts were unsuccessful and the matter came before the ECtHR. Zakharov claimed this system constituted a violation of Article 8 ECHR, which provides for the right to respect for private and family life, home, and correspondence.

## Decision

The first issue was that of standing. The ECtHR requires an applicant to be a victim within the terms of Article 34 ECHR. The difficulty in the context of secret surveillance is that the subjects of surveillance are unlikely to know that their communications are being intercepted. The ECtHR has grappled with this issue before, recognizing the particular nature of secret surveillance. The ECtHR referred to its earlier jurisprudence in which two approaches can be found:

1. the first requires proof of a "reasonable likelihood" of interception when an applicant claims that interception of the applicant's communications is claimed; and
2. the second dates back to the case of *Klass*,[3] which accepted the "threat of surveillance for all those to whom the legislation might be applied."[4]

The ECtHR sought to harmonize its approach, reflecting the point made in the case of *Kennedy*,[5] that a key issue was to ensure that such systems do not end up "being effectively unchallengeable."[6] The ECtHR accepted the principle that legislation, rather than a specific instance of interception, can be challenged if the applicant falls within the class potentially within the scope of the impugned rules, taking into consideration the availability of remedies. If there are no effective remedies, a challenge to the legislation may proceed, but even if remedies exist, an applicant can challenge the legislation if "due to his personal situation, he is potentially at risk of being subjected to such measures."[7] Here, since there were no effective remedies in the Russian system, Zakharov did not need to demonstrate that he was at specific risk of surveillance.

The ECtHR assessed the justification for the interference according to the conditions set down in Article 8(2) ECHR. Restrictions must be in accordance with the law, pursue at least one of the legitimate aims listed in Article 8(2), and be necessary in a democratic society to achieve such aims.[8]

The ECtHR reiterated its long-standing position that "in accordance with the law" requires the impugned rule to have some basis in domestic law, to be accessible to the person concerned with foreseeable effects. Given the nature of surveillance, "foreseeable" cannot mean that an individual should be able to predict specific instances of interception. Instead, an individual should be given "an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered" to carry out such interception.[9] Referring to its earlier jurisprudence, the ECtHR set out factors to be considered:

* Professor Lorna Woods is a professor in the Law School and Human Rights Centre at Essex University. Formerly a practicing solicitor in an ICT practice, she has extensive experience in the field of media policy, communications regulation, and freedom of expression and privacy, and she has published widely in these areas.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

- identification of the offences potentially triggering an interception order;
- the categories of people who may be subject to the order;
- rules on duration of surveillance;
- procedure for examining, using, or storing any data;
- precautions with respect to communicating the data to others; and
- the circumstances in which recordings may or must be erased.[10]

While critical of some aspects of the Russian system, the ECtHR accepted that this element of Article 8(2) was satisfied.[11]

The ECtHR accepted that the aims of the surveillance were legitimate. They were in the interests "of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country."[12]

The question was whether the measures were necessary, and in this the existence and effectiveness of safeguards against abuse were central. In this there were links to the question of "lawfulness." While the authorities retain some margin of appreciation, they are subject to review both in terms of the legislation itself and in respect of individual decisions. The ECtHR emphasized the need to ensure that there are adequate and effective guarantees against abuse, taking into account the circumstances of the case,[13] and that "the values of a democratic society must be followed as faithfully as possible" when supervising surveillance so the limits of necessity are not exceeded.[14]

The ECtHR assessed the Russian system according to the factors set out above, taking into account the way the system operated in practice. While judicial authorities were involved in the authorization process, it was questionable whether they verified the existence of reasonable suspicion against the person concerned and whether the surveillance was necessary in a democratic society. Notably, the magistrates were not provided, nor did they request, the information necessary to carry out this function. Authorizations often did not clearly identify the target of the surveillance. Further, the system did not distinguish unmistakably between witness and suspect, so it was unclear who could be the subject of surveillance and individuals were not notified of interception. Given the possibility of direct access to the communications network and the fact the system kept no logs of access, it was possible to bypass the legislative safeguards. Russian legislation regarding the deletion of data, especially clearly irrelevant data, did not contain adequate safeguards. Taken together, the Court determined that the system was prone to abuse and the safeguards were inadequate.[15] In sum, the Russian system was not necessary in a democratic society and the ECtHR therefore found a violation of Article 8 ECHR.

## Comment

The *Zakharov* judgment restates existing jurisprudence, though this consolidation with the authority of a Grand Chamber is welcome. Two aspects regarding legal principle should be noted. The first point is the reconciliation of diverging approaches in its previous case law to the question of standing in relation to the existence of a surveillance system. While *Klass* accepted that the menace of an overarching secret surveillance system was sufficient to show an interference with Article 8, other cases, such as *Estbester*, required a "reasonable likelihood" of surveillance.[16] Although the ECtHR in *Zakharov* may have been seeking the middle ground between the two positions, it is arguable that even should an applicant now need to show that he is at risk, the test in *Zakharov* seems to indicate a lower threshold than that set by the *Estbester* line of cases. In any event, this is a broad approach to standing.[17]

Secondly, the question of whether there are effective safeguard and oversight mechanisms is central. This theme runs through the *Zacharov* judgment. This approach has the effect of blurring the question of standing (as an admissibility claim) with the merits. Indeed, the ECtHR in *Zacharov* treated the question as one pertaining to the merits and not admissibility.[18] This may mean that it will be difficult for a state to argue that a claim is clearly inadmissible, especially where the case involves mass surveillance.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

The abstract nature of the review means two linked questions are significant: the determination of "in accordance with the law" and the question of whether the measures (rather than individual applications) are necessary in a democratic society. This leads to a close review of the system itself and its safeguards. When considering the authorization process, the question is not just who carries out that function and that body's independence, but also the scope of review and the ability of the reviewer to verify reasonable suspicion in individual cases. So, situations that allow public authorities just to restate the wording of the authorizing statute without any supporting evidence would seem to fail this test. The Court expressed concern about broadly determined definitions in the context of "national, military, economic or ecological security," which confer "an almost unlimited degree of discretion."[19]

This approach has a couple of additional consequences. The ECtHR specified that, in order for review to be thorough, an authorization should identify the specific target by name, address, or telephone number. Does this mean that mass surveillance is unlikely to satisfy this criterion? This was not directly addressed in *Zakharov* because there was no allegation that the authorities were carrying out such mass interception. In a subsequent chamber decision, *Szabó*,[20] the ECtHR appeared to accept that mass acquisition of data may be necessary but on the facts at issue the safeguards were inadequate. A concurring opinion, however, expressed a strong view that the Grand Chamber imposed a requirement for a more specific level of suspicion to justify surveillance than this.[21]

The ruling in *Zakharov* found the use of technology that allowed the security services and police access to the communications network particularly problematic. It seems that no matter what the legal system, such direct access allows the relevant public authorities a way to circumvent controls—a position that is particularly prone to abuse.[22] The ECtHR noted that "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,"[23] especially as there were no access logs. This implies a strong presumption against the legality of any "black boxes" allowing direct access, whether in the context of communications data or content. It may also affect legal provisions seeking to legitimize hacking, computer exploits, and the like.

This judgment is clearly anchored in well-known jurisprudence. Points of interest arise in the way the ECtHR applied its principles not only to the Russian system as described in its laws but also how that system operated in practice and specifically whether the safeguards against abuse were effective. Significantly, the ECtHR has drawn its judgment in terms that raise questions about the validity of other systems of mass surveillance.

## ENDNOTES

1 Zakharov v. Russia, Eur. Ct. H.R. (2015), http://hudoc.echr.coe.int/eng-press?i=001-159324.

2 See Big Brother Watch v. U.K. (application no 58170/13), Bureau of Investigative Journalism and Ross v. U.K. (application no. 62322/14), and Tretter v. Austria (application no. 3599/10), for cases on surveillance that are pending before the ECtHR.

3 Klass v. Germany, App. No. 5029/71, 2 Eur. H.R. Rep. 214 (1978).

4 Zakharov, *supra* note 1, ¶¶ 167–68.

5 Kennedy v. United Kingdom, 2010 Eur. Ct. H.R. 682.

6 Zakharov, *supra* note 1, ¶ 169.

7 *Id.* ¶ 171.

8 *Id.* ¶ 227.

9 *Id.* ¶ 229.

10 *Id.* ¶ 231.

11 *Id.* ¶ 242.

12 *Id.* ¶ 237.

13 *Id.* ¶ 232.

14 *Id.* ¶ 233.

15 *Id.* ¶ 302.

16 Esbester v. United Kingdom, 1993 Eur. Ct. H.R. 64; *see also* Halford v. United Kingdom, 1997-III Eur. Ct. H.R. 32, ¶ 17.

17 Zakharov, *supra* note 1, Concurring Opinion of Judge Dedov, ¶ 3.

18 Note that in Szabó and Vissy v. Hungary, Eur. Ct. H.R. 2016, http://hudoc.echr.coe.int/eng?i=001-160020 the ECtHR treated this as a question of admissibility, but found the matter admissible.

19 *Id.* ¶ 248.

20 Szabó and Vissy, *supra* note 18.

21 *Id.* Concurring Opinion, ¶ 20.

22 Zakharov, *supra* note 1, ¶ 269.

23 *Id.* ¶ 268.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRAND CHAMBER

**CASE OF ROMAN ZAKHAROV v. RUSSIA**

*(Application no. 47143/06)*

JUDGMENT

STRASBOURG

4 December 2015

*This judgment is final but it may be subject to editorial revision.*

**In the case of Roman Zakharov v. Russia,**

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Dean Spielmann, *President,*

Josep Casadevall,

Guido Raimondi,

Ineta Ziemele,

Mark Villiger,

Luis López Guerra,

Khanlar Hajiyev,

Angelika Nußberger,

Julia Laffranque,

Linos-Alexandre Sicilianos,

Erik Møse,

André Potocki,

Paul Lemmens,

* This text was reproduced and reformatted from the text available at the European Court of Human Rights website (visited March 14, 2016), http://hudoc.echr.coe.int/eng-press?i=001-159324#{"itemid":["001-159324"]}.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

Helena Jäderblom,

Faris Vehabović,

Ksenija Turković,

Dmitry Dedov, *judges,*

and Lawrence Early, *Jurisconsult,*

Having deliberated in private on 24 September 2014 and 15 October 2015,

Delivers the following judgment, which was adopted on the last-mentioned date:

**PROCEDURE**

1. The case originated in an application (no. 47143/06) against the Russian Federation lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Russian national, Mr Roman Andreyevich Zakharov ("the applicant"), on 20 October 2006.

2. The applicant was initially represented by Mr B. Gruzd, a lawyer practising in St Petersburg. He was subsequently represented by lawyers of the NGO EHRAC/Memorial Human Rights Centre, based in Moscow. The Russian Government ("the Government") were represented by Mr G. Matyushkin, Representative of the Russian Federation at the European Court of Human Rights.

3. The applicant alleged that the system of secret interception of mobile telephone communications in Russia violated his right to respect for his private life and correspondence and that he did not have any effective remedy in that respect.

4. On 19 October 2009 the application was communicated to the Government.

5. On 11 March 2014 the Chamber of the First Section, to which the case had been allocated (Rule 52 § 1 of the Rules of Court), composed of Isabelle Berro-Lefèvre, President, Khanlar Hajiyev, Julia Laffranque, Linos-Alexandre Sicilianos, Erik M,se, Ksenija Turković, Dmitry Dedov, judges, and also of S,ren Nielsen, Section Registrar, relinquished jurisdiction in favour of the Grand Chamber, neither of the parties having objected to relinquishment (Article 30 of the Convention and Rule 72).

6. A hearing took place in public in the Human Rights Building, Strasbourg, on 24 September 2014 (Rule 59 § 3).

There appeared before the Court:

(a) *for the Government*

Mr G. MATYUSHKIN, Representative of the Russian Federation at the European Court of Human Rights, *Agent*,

Ms O. SIROTKINA,

Ms I. KORIEVA,

Ms O. IURCHENKO,

Mr O. AFANASEV,

Mr A. LAKOV, *Advisers*;

(b) *for the applicant*

Mr P. LEACH,

Ms K. LEVINE,

Mr K. KOROTEEV,

Ms A. RAZHIKOVA, *Counsel,*

Ms E. LEVCHISHINA, *Adviser.*

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

The Court heard addresses by Mr Matyushkin, Mr Leach, Ms Levine, Ms Razhikova and Mr Koroteev, and also replies by Mr Matyushkin and Mr Leach to questions put by the judges.

**THE FACTS**

I. THE CIRCUMSTANCES OF THE CASE

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

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

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

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

11. On 5 December 2005 the Vasileostrovskiy District Court of St Petersburg dismissed the applicant's claims. It found that the applicant had not proved that the mobile network operators had transmitted any protected information to unauthorised persons or permitted the unrestricted or unauthorised interception of communications. The equipment to which he referred had been installed to enable law-enforcement agencies to conduct operational-search activities in accordance with the procedure prescribed by law. The installation of such equipment had not in itself interfered with the privacy of the applicant's communications. The applicant had failed to demonstrate any facts which would warrant a finding that his right to the privacy of his telephone communications had been violated.

12. The applicant appealed. He claimed, in particular, that the District Court had refused to accept several documents in evidence. Those documents had included two judicial orders authorising the interception of mobile telephone communications retrospectively and an addendum to the standard service provider agreement issued by one of the mobile network operators. One of the judicial orders in question, issued on 8 October 2002, authorised the interception of several people's mobile telephone communications during the periods from 1 to 5 April, from 19 to 23 June, from 30 June to 4 July and from 16 to 20 October 2001. The other judicial order, issued on 18 July 2003, authorised the interception of a Mr E.'s mobile telephone communications during the period from 11 April to 11 October 2003. As to the addendum, it informed the subscriber that if his number were used to make terrorist threats, the mobile network operator might suspend the provision of the telephone service and transfer the collected data to the law-enforcement agencies. In the applicant's opinion, the judicial orders and the addendum proved that the mobile network operators and law-enforcement agencies were technically capable of intercepting all telephone communications without obtaining prior judicial authorisation, and routinely resorted to unauthorised interception.

13. On 26 April 2006 the St Petersburg City Court upheld the judgment on appeal. It confirmed the District Court's finding that the applicant had failed to prove that his telephone communications had been intercepted. Nor had he shown that there was a danger that his right to the privacy of his telephone communications might be unlawfully infringed. To establish the existence of such a danger, the applicant would have had to prove that the respondents had acted unlawfully. However, mobile network operators were required by law to install equipment enabling law-enforcement agencies to perform operational-search activities and the existence of that equipment did not in itself interfere with the privacy of the applicant's communications. The refusal to admit the judicial orders of 8

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

October 2002 and 18 July 2003 in evidence had been lawful, as the judicial orders had been issued in respect of third persons and were irrelevant to the applicant's case. The City Court further decided to admit in evidence and examine the addendum to the service provider agreement, but found that it did not contain any information warranting reconsideration of the District Court's judgment.

14. It can be seen from a document submitted by the applicant that in January 2007 an NGO, "Civilian Control", asked the Prosecutor General's office to carry out an inspection of the Ministry of Communications' Orders in the sphere of interception of communications in order to verify their compatibility with federal laws. In February 2007 an official from the Prosecutor General's office telephoned "Civilian Control" and asked for copies of the unpublished attachments to Order No. 70, saying that the prosecutor's office had been unable to obtain them from the Ministry of Communications. In April 2007 the Prosecutor General's office refused to carry out the requested inspection.

## II. RELEVANT DOMESTIC LAW

### A. Right to respect for private life and correspondence

15. The Constitution guarantees to everyone the right to respect for his private life, personal and family secrets and the right to defend his honour and reputation (Article 23 § 1). It further guarantees the right to respect for correspondence, telephone, postal, telegraph and other communications. That right may be restricted only on the basis of a court order (Article 23 § 2).

16. The Constitution also stipulates that it is not permissible to collect, store, use or disseminate information about a person's private life without his/her consent. State and municipal authorities must ensure that any person has access to documents and materials affecting his rights and freedoms, except where the law provides otherwise (Article 24).

17. The Communications Act of 7 July 2003 (no. 126-FZ) guarantees the privacy of postal, telegraphic and other forms of communication transmitted by means of telecommunications networks or mail services. Restrictions on the privacy of communications are permissible only in cases specified in federal laws (section 63(1)). The interception of communications is subject to prior judicial authorisation, except in cases specified in federal laws (section 63(3)).

18. On 2 October 2003 in its decision no. 345-O the Constitutional Court held that the right to privacy of telephone communications covered all data transmitted, stored or discovered by means of telephone equipment, including non-content-based data, such as information about the incoming and outgoing connections of a specified subscriber. The monitoring of such data was also subject to prior judicial authorisation.

### B. Responsibility for breach of privacy

19. The unauthorised collection or dissemination of information about the private or family life of a person without his or her consent, where it is committed out of mercenary or other personal interest and is damaging to the rights and lawful interests of citizens, is punishable by a fine, correctional labour or a custodial sentence of up to four months. The same actions committed by an official using his or her position are punishable by a fine, a prohibition on occupying certain positions or a custodial sentence of up to six months (Article 137 of the Criminal Code).

20. Any breach of citizens' right to the privacy of their postal, telegraphic, telephone or other forms of communication is punishable by a fine or correctional labour. The same act committed by an official using his or her position is punishable by a fine, a prohibition on occupying certain positions or a custodial sentence of up to four months (Article 138 of the Criminal Code).

21. Abuse of power by an official, where it is committed out of mercenary or other personal interest and entails a substantial violation of an individual's or a legal entity's rights and lawful interests, is punishable by a fine, a prohibition on occupying certain posts or engaging in certain activities for a period of up to five years, correctional

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

labour for a period of up to four years or imprisonment for a period ranging from four months to four years (Article 285 § 1 of the Criminal Code).

22. Actions by a public official which clearly exceed his or her authority and entail a substantial violation of an individual's or a legal entity's rights and lawful interests, are punishable by a fine, a prohibition on occupying certain posts or engaging in certain activities for a period of up to five years, correctional labour for a period of up to four years or imprisonment for a period ranging from four months to four years (Article 286 § 1 of the Criminal Code).

23. Ruling no. 19 of 16 October 2009 by the Plenary Supreme Court provides that for the purposes of Articles 285 and 286 of the Criminal Code "a substantial violation of an individual's or a legal entity's rights and lawful interests" means a violation of the rights and freedoms guaranteed by the generally established principles and provisions of international law and the Constitution of the Russian Federation – such as the right to respect for a person's honour and dignity, private or family life, correspondence, telephone, postal, telegraph and other communications, the inviolability of the home, etc. In assessing whether the violation was "substantial" in respect of a legal entity, it is necessary to take into account the extent of the damage sustained as a result of the unlawful act, the nature and the amount of the pecuniary damage, the number of persons affected and the gravity of the physical, pecuniary or non-pecuniary damage inflicted on them (paragraph 18 (2)).

24. Criminal proceedings are opened if there are sufficient facts showing that a criminal offence has been committed (Article 140 § 2 of the Code of Criminal Procedure).

### C. General provisions on interception of communications

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

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

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

28. State officials and agencies may not (1) conduct operational-search activities in the interest of political parties, non-profit or religious organisations; (2) conduct secret operational-search activities in respect of federal, regional or municipal authorities, political parties, or non-profit or religious organisations with the aim of influencing their activities or decisions; (3) disclose to anyone the data collected in the course of the operational-search activities if that data concern the private or family life of citizens or damage their reputation or good name, except in cases specified in federal laws; (4) incite, induce or entrap anyone to commit a criminal offence; (5) falsify the results of operational-search activities (section 5(8) of the OSAA).

29. Operational-search activities include*, inter alia*, the interception of postal, telegraphic, telephone and other forms of communication and the collection of data from technical channels of communication. The Act stipulates that audio and video recording, photography, filming and other technical means may be used during operational-search activities, provided that they are not harmful to the life or health of those involved or to the environment. Operational-search activities involving the interception of postal, telegraphic, telephone and other forms of communication and collection of data from technical channels of communication using equipment installed by communications service providers is carried out by technical means by the FSB and the agencies of the Ministry of the

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

Interior, in accordance with decisions and agreements signed between the agencies involved (section 6 of the OSAA).

30. Presidential Decree no. 891 of 1 September 1995 provides that the interception of postal, telegraphic or other communications is to be carried out by the FSB in the interests and on behalf of all law-enforcement agencies (paragraph 1). In situations where the FSB does not have available the necessary technical equipment, interceptions may be carried out by the agencies of the Ministry of the Interior in the interests and on behalf of all law-enforcement agencies (paragraph 2). Similar provisions are contained in paragraphs 2 and 3 of Order no. 538, issued by the Government on 27 August 2005.

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

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

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

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

### E. Authorisation procedure and time-limits

#### *1. Operational-Search Activities Act*

34. Operational-search measures involving interference with the constitutional right to the privacy of postal, telegraphic and other communications transmitted by means of a telecommunications network or mail services or within the privacy of the home – such as an inspection of premises or buildings, an interception of postal, telegraphic, telephone and other forms of communication or a collection of data from technical channels of communication – require prior judicial authorisation (section 8(2) of the OSAA).

35. In urgent cases where there is an immediate danger that a serious or especially serious offence may be committed or where there is information about events or activities endangering national, military, economic or ecological security, the operational-search measures specified in section 8(2) may be conducted without prior judicial authorisation. In such cases a judge must be informed within twenty-four hours of the commencement of the operational-search activities. If judicial authorisation has not been obtained within forty-eight hours of the commencement of the operational-search activities, those activities must be stopped immediately (section 8(3) of the Act).

36. The examination of requests to take measures involving interference with the constitutional right to the privacy of correspondence and telephone, postal, telegraphic and other communications transmitted by means of telecommunications networks or mail services, or with the right to privacy of the home, falls within the competence

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

of a court in the locality where the requested measure is to be carried out or in the locality where the requesting body is located. The request must be examined immediately by a single judge (section 9(1) of the Act).

37. The judge takes a decision on the basis of a reasoned request by the head of one of the agencies competent to perform operational-search activities. Relevant supporting materials, except materials containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures, may also be produced at the judge's request (section 9(2) and (3) of the Act).

38. The judge examining the request shall decide whether to authorise measures involving interference with the above-mentioned constitutional rights, or to refuse authorisation, giving reasons. The judge must specify the period of time for which the authorisation is granted, which shall not normally exceed six months. If necessary, the judge may extend the authorised period after a fresh examination of all the relevant materials (section 9(4) and (5) of the Act).

39. The judicial decision authorising operational-search activities and the materials that served as a basis for that decision must be held in the exclusive possession of the State agency performing the operational-search activities (section 12(3) of the Act).

40. On 14 July 1998 the Constitutional Court, in its decision no. 86-O, dismissed as inadmissible a request for a review of the constitutionality of certain provisions of the OSAA. It held, in particular, that a judge was to authorise investigative measures involving interference with constitutional rights only if he or she was persuaded that such measures were lawful, necessary and justified, that is, compatible with all the requirements of the OSAA. The burden of proof was on the requesting State agency to show the necessity of the measures. Supporting materials were to be produced to the judge at his or her request. Given that some of those materials might contain State secrets, only judges with the necessary level of security clearance could examine authorisation requests. Further, relying on the need to keep the surveillance measures secret, the Constitutional Court held that the principles of a public hearing and adversarial proceedings were not applicable to the authorisation proceedings. The fact that the person concerned was not entitled to participate in the authorisation proceedings, to be informed about the decision taken or to appeal to a higher court did not therefore violate that person's constitutional rights.

41. On 2 October 2003 the Constitutional Court, in its decision no. 345-O, held that the judge had an obligation to examine the materials submitted to him or her in support of a request for interception thoroughly and carefully. If the request was insufficiently substantiated, the judge might request additional information.

42. Further, on 8 February 2007 the Constitutional Court, in its decision no. 1-O, dismissed as inadmissible a request for a review of the constitutionality of section 9 of the OSAA. The Court found that before granting authorisation to perform operational-search measures the judge had an obligation to verify the grounds for that measure. The judicial decision authorising operational-search measures was to contain reasons and to refer to specific grounds for suspecting that a criminal offence had been committed, or was ongoing, or was being plotted or that activities endangering national, military, economic or ecological security were being carried out, and that the person in respect of whom operational-search measures were requested was involved in those criminal or otherwise dangerous activities.

43. On 15 July 2008 the Constitutional Court, in its decision no. 460-O-O, dismissed as inadmissible a request for a review of the constitutionality of sections 5, 11 and 12 of the OSAA. The Constitutional Court found that the person whose communications had been intercepted was entitled to lodge a supervisory review complaint against the judicial decision authorising the interception. The fact that he had no copy of that decision did not prevent him from lodging the supervisory-review complaint, because the relevant court could request it from the competent authorities.

### *2. Code of Criminal Procedure*

44. Investigative measures involving a search in a person's home or interception of his or her telephone calls and other communications are subject to prior judicial authorisation. A request to search a person's home or intercept his or her communications must be submitted by an investigator with a prosecutor's approval and must be examined by a single judge within twenty-four hours. The prosecutor and the investigator are entitled to attend. The judge

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

examining the request shall decide whether to authorise the requested measure, or to refuse authorisation, giving reasons (Article 165 of the CCrP).

45. A court may grant authorisation to intercept the communications of a suspect, an accused or other persons if there are reasons to believe that information relevant to the criminal case may be discussed (Article 186 § 1 of the CCrP).

46. A request for authorisation to intercept communications must clearly mention the following: (1) the criminal case to which the request is related; (2) the grounds for conducting the requested measures; (3) the family name, the first name and the patronymic of the person whose communications are to be intercepted; (4) the duration of the requested measure; (5) the State agency that will perform the interception (Article 186 § 3 of the CCrP).

47. The judicial decision authorising interception of communications must be forwarded by the investigator to the State agency charged with its implementation. The interception of communications may be authorised for a period not exceeding six months, and is discontinued by the investigator when it is no longer necessary. It must in any case be discontinued when the investigation has been completed (Article 186 §§ 4 and 5 of the CCrP).

48. A court may also authorise the monitoring of communications data relating to a person's telephone or wireless connections if there are sufficient reasons to believe that such data may be relevant to a criminal case. A request for authorisation must contain the same elements referred to in paragraph 46 above. A copy of the judicial decision authorising the monitoring of a person's communications-related data is forwarded by the investigator to the relevant communications service provider, which must then submit the requested data to the investigator on a regular basis, and at least once a week. The monitoring of communications data may be authorised for a period not exceeding six months, and is discontinued by the investigator when it is no longer necessary. It must in any case be discontinued when the investigation has been completed (Article 186.1 of the CCrP, added on 1 July 2010).

### F. Storage, use and destruction of collected data

#### *1. Storage of collected data*

49. Section 10 of the OSAA stipulates that law-enforcement agencies performing operational-search activities may create and use databases or open personal files. The personal file must be closed when the aims specified in section 2 of the Act have been achieved or if it has been established that it is impossible to achieve them.

50. In its decision of 14 July 1998 (cited in paragraph 40 above) the Constitutional Court noted, as regards the possibility provided by section 10 for law-enforcement agencies conducting operational-search activities to create databases or open personal files, that only the data relating to the prevention or investigation of criminal offences could be entered into such databases or personal files. Given that criminal activities did not fall within the sphere of private life, collection of information about such criminal activities did not interfere with the right to respect for private life. If information about a person's criminal activities entered into a file was not subsequently confirmed, the personal file had to be closed.

51. Records of intercepted telephone and other communications must be sealed and stored under conditions excluding any risk of their being listened to or copied by unauthorised persons (section 8(4) of the OSAA).

52. Information about the facilities used in operational-search activities, the methods employed, the officials involved and the data collected constitutes a State secret. It may be declassified only pursuant to a special decision of the head of the State agency performing the operational-search activities (section 12(1) of the OSAA and section 5(4) of the State Secrets Act, Law no. 5485-I of 21 July 1993).

53. Materials containing State secrets should be clearly marked with the following information: degree of secrecy, the State agency which has taken the decision to classify them, registration number, and the date or conditions for declassifying them (section 12 of the State Secrets Act).

#### *2. Use of collected data and conditions for their disclosure*

54. Information containing State secrets may be disclosed to another State authority, an organisation or an individual only subject to authorisation by the State authority which took the decision to classify that information. It

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

may be disclosed only to State authorities or organisations holding a special license or to individuals with the required level of security clearance. The State authority or organisation to which classified information is disclosed must ensure that that information is adequately protected. The head of such State authority or organisation is personally responsible for protecting the classified information against unauthorised access or disclosure (sections 16 and 17 of the State Secrets Act).

55. A license to access State secrets may be issued to an organisation or a company only after it has been confirmed that it has specific internal sections charged with data protection, that its employees are qualified to work with classified information and that it uses approved systems of data protection (section 27 of the State Secrets Act).

56. Security clearance is granted only to those state officials who genuinely need it for the performance of their duties. It is also granted to judges for the period of their service and to counsel participating in a criminal case if the case-file contains materials involving State secrets. Anyone who has been granted security clearance must give a written undertaking not to disclose the classified information entrusted to him or her (paragraphs 7, 11 and 21 of Regulation no. 63 of 6 February 2010 of the Government of the Russian Federation).

57. The head of the State authority or organisation in possession of information containing State secrets is responsible for giving State officials and other authorised persons access to that information. He or she must ensure that only the information that the recipient needs for the performance of his or her duties is disclosed (section 25 of the State Secrets Act).

58. If the data collected in the course of operational-search activities contain information about the commission of a criminal offence, that information, together with all the necessary supporting material such as photographs and audio or video recordings, must be sent to the competent investigation authorities or a court. If the information was obtained as a result of operational-search measures involving interference with the right to the privacy of postal, telegraphic and other communications transmitted by means of a telecommunications network or mail services, or with the privacy of the home, it must be sent to the investigation or prosecution authorities together with the judicial decision authorising those measures. The information must be transmitted in accordance with the special procedure for handling classified information, unless the State agency performing operational-search activities has decided to declassify it (paragraphs 1, 12, 14 and 16 of Order no. 776/703/509/507/1820/42/535/398/68 of 27 September 2013 by the Ministry of the Interior).

59. If the person whose telephone or other communications were intercepted is charged with a criminal offence, the records are to be given to the investigator and attached to the criminal case file. Their further use and storage are governed by criminal procedural law (section 8(5) of the OSAA).

60. Data collected as a result of operational-search activities may be used for the preparation and conduct of the investigation and court proceedings and used as evidence in criminal proceedings in accordance with the legal provisions governing the collection, evaluation and assessment of evidence. The decision to transfer the collected data to other law-enforcement agencies or to a court is taken by the head of the State agency performing the operational-search activities (section 11 of the OSAA).

61. If the interception was authorised in the framework of criminal proceedings, the investigator may obtain the records from the agency conducting it at any time during the authorised period of interception. The records must be sealed and must be accompanied by a cover letter indicating the dates and time of the beginning and end of the recorded communications, as well as the technical means used to intercept them. Recordings must be listened to by the investigator in the presence of attesting witnesses, an expert where necessary and the persons whose communications have been intercepted. The investigator must draw up an official report containing a verbatim transcription of those parts of the recorded communications that are relevant to the criminal case (Article 186 §§ 6 and 7 of the CCrP). On 4 March 2013 Article 186 § 7 was amended and the requirement of the presence of attesting witnesses was deleted.

62. Recordings and communications-related data collected are to be attached to the criminal case file. They must be sealed and stored under conditions excluding any risk of their being listened to or copied by unauthorised persons (Article 186 § 8 of the CCrP and Article 186.1, added on 1 July 2010).

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

63. The results of operational-search activities involving a restriction on the right to respect for correspondence, telephone, postal, telegraph or other communications may be used as evidence in criminal proceedings only if they have been obtained pursuant to a court order and if the operational-search activities have been carried out in accordance with the law on criminal procedure (paragraph 14 of Ruling no. 8 of 31 October 1995 by the Plenary Supreme Court of the Russian Federation).

64. It is prohibited to use in evidence data, obtained as a result of operational-search activities, which do not comply with the admissibility-of-evidence requirements of the CCrP (Article 89 of the CCrP). Evidence obtained in breach of the CCrP shall be inadmissible. Inadmissible evidence shall have no legal force and cannot be relied on as grounds for criminal charges or for proving any of the circumstances for which evidence is required in criminal proceedings. If a court decides to exclude evidence, that evidence shall have no legal force and cannot be relied on in a judgment or other judicial decision, or be examined or used during the trial (Articles 75 and 235 of the CCrP).

*3. Destruction of collected data*

65. The data collected in the course of operational-search activities in respect of a person whose guilt has not been proved in accordance with the procedure prescribed by law must be stored for a year and then destroyed, unless that data are needed in the interests of the service or justice. Audio recordings and other materials collected as a result of intercepting telephone or other communications must be stored for six months and then destroyed if the person has not been charged with a criminal offence. The judge who authorised the interception must be informed of the scheduled destruction three months in advance (section 5(7) of the OSAA).

66. If the person has been charged with a criminal offence, at the end of the criminal proceedings the trial court takes a decision on the further storage or destruction of the data used in evidence. The destruction must be recorded in a report to be signed by the head of the investigation authority and included in the case file (Article 81 § 3 of the CCrP and paragraph 49 of Order no. 142 of 30 September 2011 of the Investigations Committee).

### G. Supervision of interception of communications

67. The heads of the agencies conducting operational-search activities are personally responsible for the lawfulness of all operational-search activities (section 22 of the OSAA).

68. Overall supervision of operational-search activities is exercised by the President, the Parliament and the Government of the Russian Federation within the limits of their competence (section 20 of the OSAA).

69. The Prosecutor General and competent lower-level prosecutors may also exercise supervision over operational-search activities. At the request of a competent prosecutor, the head of a State agency performing operational-search activities must produce operational-search materials, including personal files, information on the use of technical equipment, registration logs and internal instructions. Materials containing information about undercover agents or police informers may be disclosed to the prosecutor only with the agent's or informer's consent, except in cases of criminal proceedings against them. The head of a State agency may be held liable in accordance with the law for failure to comply with the prosecutor's request. The prosecutor must ensure the protection of the data contained in the materials produced (section 21 of the OSAA).

70. The Prosecutors' Office Act (Federal law no. 2202-I of 17 January 1992) provides that the Prosecutor General is to be appointed or dismissed by the Federation Council (the upper house of the Parliament) on proposal by the President (section 12). Lower-level prosecutors are to be appointed by the Prosecutor General after consultation with the regional executive authorities (section 13). To be appointed as a prosecutor the person must be a Russian citizen and must have a Russian law degree (section 40.1).

71. In addition to their prosecuting functions, prosecutors are responsible for supervising whether the administration of detention facilities, bailiffs' activities, operational-search activities and criminal investigations are in compliance with the Russian Constitution and Russian laws (section 1). Prosecutors also coordinate the activities of all law-enforcement authorities in combatting crime (section 8).

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

72. As regards supervision of operational-search activities, prosecutors may review whether measures taken in the course of operational-search activities are lawful and respectful of human rights (section 29). Prosecutors' orders made in the context of such supervision must be complied with within the time-limit set. Failure to comply may result in liability in accordance with the law (section 6).

73. Prosecutors may also examine complaints of breaches of the law and give a reasoned decision on each complaint. Such a decision does not prevent the complainant from bringing the same complaint before a court. If a prosecutor discovers a breach of the law, he or she must take measures to bring the responsible persons to liability (section 10).

74. The Federal Security Service Act of 3 April 1995 (no. 40-FZ, hereafter "the FSB Act") provides that information about the security services' undercover agents, as well as about the tactics, methods and means used by them is outside the scope of supervision by prosecutors (section 24).

75. The procedures for prosecutors' supervision of operational-search activities have been set out in Order no. 33, issued by the Prosecutor General's Office on 15 February 2011.

76. Order no. 33 provides that a prosecutor may carry out routine inspections of agencies carrying out operational-search activities, as well as *ad hoc* inspections following a complaint by an individual or receipt of information about potential violations. Operational-search activities performed by the FSB in the sphere of counter-intelligence may be inspected only following an individual complaint (paragraph 5 of Order no. 33).

77. During the inspection the prosecutor must verify compliance with the following requirements:

- observance of citizens' constitutional rights, such as the right to respect for private and family life, home, correspondence, telephone, postal, telegraph and other communications;

- that the measures taken in the course of operational-search activities are lawful and justified, including those measures that have been authorised by a court (paragraphs 4 and 6 of Order no. 33).

78. During the inspection the prosecutor must study the originals of the relevant operational-search materials, including personal files, information on the use of technical equipment, registration logs and internal instructions, and may request explanations from competent officials. The prosecutors must protect the sensitive data entrusted to them from unauthorised access or disclosure (paragraphs 9 and 12 of Order no. 33).

79. If a prosecutor identifies a breach of the law, he or she must request the official responsible for it to remedy the breach. He or she must also take measures to stop and remedy violations of citizens' rights and to bring those responsible to liability (paragraphs 9 and 10 of Order no. 33). A State official who refuses to comply with a prosecutor's orders may be brought to liability in accordance with the law (paragraph 11).

80. The prosecutors responsible for supervision of operational-search activities must submit six-monthly reports detailing the results of the inspections to the Prosecutor General's Office (paragraph 15 of Order no. 33). A report form to be filled by prosecutors is attached to Order no. 33. The form indicates that it is confidential. It contains two sections, both in table format. The first section concerns inspections carried out during the reference period and contains information about the number of inspections, number of files inspected and number of breaches detected. The second section concerns citizens' complaints and contains information about the number of complaints examined and granted.

### H. Access by individuals to data collected about them in the course of interception of communications

81. Russian law does not provide that a person whose communications are intercepted must be notified at any point. However, a person who is in possession of the facts of the operational-search measures to which he or she was subjected and whose 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, is entitled to receive information about the data collected in the course of the operational-search activities, to the extent compatible with the requirements

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

of operational confidentiality ("*конспирации*") and excluding data which could enable State secrets to be disclosed (section 5(4-6) of the OSAA).

82. In its decision of 14 July 1998 (cited in paragraph 40 above) the Constitutional Court noted that any person who was in possession of the facts of the operational-search measures to which he or she had been subjected was entitled to receive information about the data collected in the course of those activities, unless that data contained State secrets. Under section 12 of the OSAA, data collected in the course of operational-search activities – such as information about criminal offences and the persons involved in their commission – were a State secret. However, information about breaches of citizens' rights or unlawful acts on the part of the authorities could not be classified as a State secret and should be disclosed. Section 12 could not therefore serve as a basis for refusing access to information affecting a person's rights, provided that such information did not concern the aims of, or the grounds for, the operational-search activities. In view of the above, the fact that, pursuant to the contested Act, a person was not entitled to be granted access to the entirety of the data collected about him or her did not constitute a violation of that person's constitutional rights.

## I. Judicial review

### *1. General provisions on judicial review of interception of communications as established by the OSAA*

83. 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. If a citizen's rights were violated in the course of operational-search activities by a State official, the official's superior, a prosecutor or a court must take measures to remedy the violation and compensate the damage (section 5(3) and (9) of the OSAA).

84. If a person was refused access to information about the data collected about him or her in the course of operational-search activities, he or she is entitled to know the reasons for the refusal of access and may appeal against the refusal to a court. The burden of proof is on the law-enforcement authorities to show that the refusal of access is justified. To ensure a full and thorough judicial examination, the law-enforcement agency responsible for the operational-search activities must produce, at the judge's request, operational-search materials containing information about the data to which access was refused, with the exception of materials containing information about undercover agents or police informers. If the court finds that the refusal to grant access was unjustified, it may compel the law-enforcement agency to disclose the materials to the person concerned (section 5(4 to 6) of the OSAA).

85. In its decision of 14 July 1998 (cited in paragraph 40 above) the Constitutional Court noted that a person who learned that he or she had been subjected to operational-search activities and believed that the actions of State officials had violated his or her rights was entitled, under section 5 of the OSAA, to challenge before a court the grounds for conducting such activities, as well as the specific actions performed by the competent authorities in the course of such activities, including in those cases where they had been authorised by a court.

86. As regards procedural matters, the Constitutional Court held that in proceedings in which the grounds for the operational-search activities or the actions of the competent authorities conducting such activities were challenged, as well as proceedings against the refusal to give access to the data collected, the law-enforcement authorities were to submit to the judge, at his or her request, all relevant operational-search materials, except materials containing information about undercover agents or police informers.

87. A person wishing to complain about interception of his or her communications may lodge a judicial review complaint under Article 125 of the CCrP; a judicial review complaint under Chapter 25 of the Code of Civil Procedure and the Judicial Review Act replaced, as from 15 September 2015, by the Code of Administrative Procedure; or a civil tort claim under Article 1069 of the Civil Code.

### *2. A judicial review complaint under Article 125 of the CCrP*

88. The Plenary Supreme Court in its Ruling no. 1 of 10 February 2009 held that actions of officials or State agencies conducting operational-search activities at the request of an investigator could be challenged in accordance

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

with the procedure prescribed by Article 125 of the CCrP (paragraph 4). The complaints lodged under that Article may be examined only while the criminal investigation is pending. If the case has already been transmitted to a court for trial, the judge declares the complaint inadmissible and explains to the complainant that he or she may raise the complaints before the relevant trial court (paragraph 9).

89. Article 125 of the CCrP provides for the judicial review of decisions and acts or failures to act by an investigator or a prosecutor which are capable of adversely affecting the constitutional rights or freedoms of the participants to criminal proceedings. The lodging of a complaint does not suspend the challenged decision or act, unless the investigator, the prosecutor, or the court decides otherwise. The court must examine the complaint within five days. The complainant, his counsel, the investigator and the prosecutor are entitled to attend the hearing. The complainant must substantiate his complaint (Article 125 §§ 1-4 of the CCrP).

90. Participants in the hearing are entitled to study all the materials submitted to the court and to submit additional materials relevant to the complaint. Disclosure of criminal-case materials is permissible only if it is not contrary to the interests of the investigation and does not breach the rights of the participants in the criminal proceedings. The judge may request the parties to produce the materials which served as a basis for the contested decision or any other relevant materials (paragraph 12 of Ruling no. 1 of 10 February 2009 of the Plenary Supreme Court of the Russian Federation).

91. Following the examination of the complaint, the court either declares the challenged decision, act or failure to act unlawful or unjustified and instructs the responsible official to rectify the indicated shortcoming, or dismisses the complaint (Article 125 § 5 of the CCrP). When instructing the official to rectify the indicated shortcoming, the court may not indicate any specific measures to be taken by the official or annul or order that the official annul the decision found to be unlawful or unjustified (paragraph 21 of Ruling no. 1 of 10 February 2009 of the Plenary Supreme Court of the Russian Federation).

*3. A judicial review complaint under Chapter 25 of the Code of Civil Procedure, the Judicial Review Act and the Code of Administrative Procedure*

92. Ruling no. 2 of 10 February 2009 of the Plenary Supreme Court of the Russian Federation provides that complaints about decisions and acts of officials or agencies performing operational-search activities that may not be challenged in criminal proceedings, as well as complaints about a refusal of access to information about the data collected in the course of operational-search activities, may be examined in accordance with the procedure established by Chapter 25 of the Code of Civil Procedure (paragraph 7).

93. Chapter 25 of the Code of Civil Procedure (the CCP), in force until 15 September 2015, established the procedure for examining complaints against decisions and acts of officials violating citizens' rights and freedoms, which was further detailed in the Judicial Review Act (Law no. 4866-1 of 27 April 1993 on Judicial review of decisions and acts violating citizens' rights and freedoms). On 15 September 2015 Chapter 25 of the CCP and the Judicial Review Act were repealed and replaced by the Code of Administrative Procedure (Law no. 21-FZ of 8 March 2015, hereafter "the CAP") which entered into force on that date. The CAP confirmed in substance and expounded the provisions of Chapter 25 of the CCP and the Judicial Review Act.

94. The CCP, the Judicial Review Act and the CAP all provide that a citizen may lodge a complaint before a court about an act or decision by any State or municipal authority or official if he considers that it has violated his rights and freedoms (Article 254 of the CCP and section 1 of the Judicial Review Act). The complaint may concern any decision, act or omission which has violated the citizen's rights or freedoms, has impeded the exercise of rights or freedoms, or has imposed a duty or liability on him (Article 255 of the CCP, section 2 of the Judicial Review Act and Article 218 § 1 of the CAP).

95. The complaint must be lodged with a court of general jurisdiction within three months of the date on which the complainant learnt of the breach of his rights. The time-limit may be extended for valid reasons (Article 254 of the CCP, sections 4 and 5 of the Judicial Review Act and Articles 218 § 5 and 219 §§ 1 and 7 of the CAP). The complaint must mention the identification number and the date of the contested decision or the date and place of commission of the contested act (Article 220 § 2 (3) of the CAP). The claimant must submit confirming documents

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

or explain why he or she is unable to submit them (Article 220 §§ 2 (8) and 3 of the CAP). If the claimant does not meet the above requirements, the judge declares the complaint inadmissible (Article 222 § 3 of the CAP).

96. The burden of proof as to the lawfulness of the contested decision, act or omission lies with the authority or official concerned. The complainant must, however, prove that his rights and freedoms were breached by the contested decision, act or omission (section 6 of the Judicial Review Act and Article 226 § 11 of the CAP).

97. Under the CCP the complaint had to be examined within ten days (Article 257 of the CCP), while under the CAP it must be examined within two months (Article 226 § 1 of the CAP). If the court finds the complaint justified, it issues a decision annulling the contested decision or act and requiring the authority or official to remedy in full the breach of the citizen's rights (Article 258 § 1 of the CCP, section 7 of the Judicial Review Act and Article 227 §§ 2 and 3 of the CAP). The court may determine the time-limit for remedying the violation and/or the specific steps which need to be taken to remedy the violation in full (paragraph 28 of Ruling no. 2 of 10 February 2009 of the Plenary Supreme Court of the Russian Federation and Article 227 § 3 of the CAP). The claimant may then claim compensation in respect of pecuniary and non-pecuniary damage in separate civil proceedings (section 7 of the Judicial Review Act).

98. The court may reject the complaint if it finds that the challenged act or decision has been taken by a competent authority or official, is lawful and does not breach the citizen's rights (Article 258 § 4 of the CCP and Articles 226 § 9 and 227 § 2 of the CAP).

99. A party to the proceedings may lodge an appeal with a higher court (Article 336 of the CCP as in force until 1 January 2012, Article 320 of the CCP as in force after 1 January 2012, and Article 228 of the CAP). The appeal decision enters into force on the day of its delivery (Article 367 of the CCP as in force until 1 January 2012, Article 329 § 5 as in force after 1 January 2012, and Articles 186 and 227 § 5 of the CAP).

100. The CCP provided that a judicial decision allowing a complaint and requiring the authority or official to remedy the breach of the citizen's rights had to be dispatched to the head of the authority concerned, to the official concerned or to their superiors within three days of its entry into force (Article 258 § 2 of the CCP). The Judicial Review Act required that the judicial decision be dispatched within ten days of its entry into force (section 8). The CAP requires that the judicial decision be dispatched on the day of its entry into force (Article 227 § 7). The court and the complainant must be notified of the enforcement of the decision no later than one month after its receipt (Article 258 § 3 of the CCP, section 8 of the Judicial Review Act and Article 227 § 9 of the CAP).

*4. A tort claim under Article 1069 the Civil Code*

101. Damage caused to the person or property of a citizen shall be compensated in full by the tortfeasor. The tortfeasor is not liable for damage if he or she proves that the damage has been caused through no fault of his or her own (Article 1064 §§ 1 and 2 of the Civil Code).

102. State and municipal bodies and officials shall be liable for damage caused to a citizen by their unlawful actions or omissions (Article 1069 of the Civil Code). Irrespective of any fault by State officials, the State or regional treasury is liable for damage sustained by a citizen on account of (i) unlawful criminal conviction or prosecution; (ii) unlawful application of a preventive measure, and (iii) unlawful administrative punishment (Article 1070 of the Civil Code).

103. A court may impose on the tortfeasor an obligation to compensate non-pecuniary damage (physical or mental suffering). Compensation for non-pecuniary damage is unrelated to any award in respect of pecuniary damage (Articles 151 § 1 and 1099 of the Civil Code). The amount of compensation is determined by reference to the gravity of the tortfeasor's fault and other significant circumstances. The court also takes into account the extent of physical or mental suffering in relation to the victim's individual characteristics (Article 151 § 2 and Article 1101 of the Civil Code).

104. Irrespective of the tortfeasor's fault, non-pecuniary damage shall be compensated for if the damage was caused (i) by a hazardous device; (ii) in the event of unlawful conviction or prosecution or unlawful application

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

of a preventive measure or unlawful administrative punishment, and (iii) through dissemination of information which was damaging to honour, dignity or reputation (Article 1100 of the Civil Code).

105. In civil proceedings a party who alleges something must prove that allegation, unless provided otherwise by Federal Law (Article 56 § 1 of the CCP).

#### *5. A complaint to the Constitutional Court*

106. The Constitutional Court Act (Law no. 1-FKZ of 21 July 1994) provides that the Constitutional Court's opinion as to whether the interpretation of a legislative provision adopted by judicial and other law-enforcement practice is compatible with the Constitution, when that opinion is expressed in a judgment, must be followed by the courts and law-enforcement authorities from the date of that judgment's delivery (section 79 (5)).

### J. Obligations of communications service providers

#### *1. Obligation to protect personal data and privacy of communications*

107. The Communications Act provides that communications service providers must ensure privacy of communications. Information about the communications transmitted by means of telecommunications networks or mail services, and the contents of those communications may be disclosed only to the sender and the addressee or their authorised representatives, except in cases specified in federal laws (section 63(2) and (4) of the Communications Act).

108. Information about subscribers and the services provided to them is confidential. Information about subscribers includes their family names, first names, patronymics and nicknames for natural persons; company names and family names, first names and patronymics of company directors and employees for legal persons; subscribers' addresses, numbers and other information permitting identification of the subscriber or his terminal equipment; data from payment databases, including information about the subscribers' communications, traffic and payments. Information about subscribers may not be disclosed to third persons without the subscriber's consent, except in cases specified in federal laws (section 53 of the Communications Act).

#### *2. Obligation to co-operate with law-enforcement authorities*

109. The Communications Act imposes an obligation on communications service providers to furnish to the law-enforcement agencies, in cases specified in federal laws, information about subscribers and services received by them and any other information they require in order to achieve their aims and objectives (section 64(1) of the Communications Act).

110. On 31 March 2008 the Moscow City Council discussed a proposal to introduce an amendment to section 64(1) of the Communications Act requiring law-enforcement agencies to show judicial authorisation to communications service providers when requesting information about subscribers. The representatives of the FSB and the Ministry of the Interior informed those present that judicial decisions authorising interceptions were classified documents and could not therefore be shown to communications service providers. The proposal to introduce the amendment was later rejected.

111. Communications service providers must ensure that their networks and equipment comply with the technical requirements developed by the Ministry of Communications in cooperation with law-enforcement agencies. Communications service providers must also ensure that the methods and tactics employed by law-enforcement agencies remain confidential (section 64(2) of the Communications Act).

112. In cases specified in federal laws communications service providers must suspend provision of service to a subscriber upon receipt of a reasoned written order by the head of a law-enforcement agency conducting operational-search activities or protecting national security (section 64(3) of the Communications Act).

113. The FSB Act requires communications service providers to install equipment permitting the FSB to carry out operational-search activities (section 15).

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

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

**(a) Order no. 70**

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

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

117. More precisely, the equipment must ensure (a) interception of all the incoming and outgoing calls of the interception subject; (b) access to information about his or her whereabouts; (c) maintenance of interception capability where an ongoing connection is transferred between the networks of different mobile network operators; (d) maintenance of interception capability in cases involving supplementary services, such as call forwarding, call transfer or conference calls, with the possibility of registering the number or numbers to which the call is routed; (e) collection of communications data concerning all types of connections, including fax, short messaging (SMS) or other; (f) access to information about the services provided to the interception subject (paragraph 2.1.2 of Addendum no. 1).

118. There are two types of interception: "total interception" and "statistical monitoring". Total interception is the real-time interception of communications data and of the contents of all communications to or by the interception subject. Statistical monitoring is real-time monitoring of communications data only, with no interception of the content of communications. Communications data include the telephone number called, the start and end times of the connection, supplementary services used, location of the interception subject and his or her connection status (paragraphs 2.2 and 2.4 of Addendum no. 1).

119. The equipment installed must be capable of launching the interception of communications within thirty seconds of receiving a command from the remote-control terminal (paragraph 2.5 of Addendum no. 1).

120. Information about interception subjects or about the transmittal of any data to the remote-control terminal cannot be logged or recorded (paragraph 5.4 of Addendum no. 1).

121. The remote-control terminal receives a password from the mobile network operator giving it full access to the SORM. The remote-control terminal then changes the password so that unauthorized persons cannot gain access to the SORM. From the remote-control terminal, the SORM can be commanded, among others, to start interception in respect of a subscriber, interrupt or discontinue the interception, intercept a subscriber's ongoing communication, and submit specified information about a subscriber (paragraph 3.1.2 of Addendum no. 3).

122. The remote-control centre receives the following automatic notifications about the interception subjects: short messages (SMS) sent or received by the interception subject, including their contents; a number being dialled;

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

a connection being established; a connection being interrupted; use of supplementary services; a change in the subject's connection status or location (paragraphs 3.1.4 of Addendum no. 3).

### (b) Order no. 130

123. Order no. 130 on the installation procedures for technical facilities enabling the conduct of operational-search activities, issued by the Ministry of Communications on 25 July 2000, stipulated that communications service providers had to install equipment which met the technical requirements laid down in Order no. 70. The installation procedure and schedule had to be approved by the FSB (paragraph 1.4).

124. Communications service providers had to take measures to protect information regarding the methods and tactics employed in operational-search activities (paragraph 2.4).

125. Communications service providers had to ensure that any interception of communications or access to communications data was granted only pursuant to a court order and in accordance with the procedure established by the OSAA (paragraph 2.5).

126. Communications service providers did not have to be informed about interceptions in respect of their subscribers. Nor did they have to be provided with judicial orders authorising interceptions (paragraph 2.6).

127. Interceptions were carried out by the staff and technical facilities of the FSB and the agencies of the Ministry of the Interior (paragraph 2.7).

128. Paragraphs 1.4 and 2.6 of Order no. 130 were challenged by a Mr N. before the Supreme Court. Mr N. argued that the reference to Order no. 70 contained in paragraph 1.4 was unlawful, as Order no. 70 had not been published and was invalid. As to paragraph 2.6, it was incompatible with the Communications Act, which provided that communications service providers had an obligation to ensure the privacy of communications. On 25 September 2000 the Supreme Court found that the reference to Order no. 70 in paragraph 1.4 was lawful, as Order no. 70 was technical in nature and was therefore not subject to publication in a generally accessible official publication**.** It had therefore been published only in a specialised magazine. As to paragraph 2.6, the Supreme Court considered that it could be interpreted as requiring communications service providers to grant law-enforcement agencies access to information about subscribers without judicial authorisation. Such a requirement was, however, incompatible with the Communications Act. The Supreme Court therefore found that paragraph 2.6 was unlawful and inapplicable.

129. On 25 October 2000 the Ministry of Communications amended Order no. 130 by repealing paragraph 2.6.

130. In reply to a request for information by the NGO "Civilian Control", the Ministry of Communications stated, in a letter dated 20 August 2006, that the repealing of paragraph 2.6 of Order no. 130 did not mean that communications service providers had to be informed about operational-search measures in respect of a subscriber or be provided with a copy of the relevant decision granting judicial authorisation for such surveillance.

131. Order no. 130 was repealed on 16 January 2008 (see paragraph 134 below).

### (c) Order no. 538

132. Order no. 538 on cooperation between communications service providers and law enforcement agencies, issued by the Government on 27 August 2005, provides that communications service providers must be diligent in updating databases containing information about subscribers and the services provided to them. That information must be stored for three years. Law-enforcement agencies must have remote access to the databases at all times (paragraph 12).

133. Databases must contain the following information about subscribers: (a) first name, patronymic and family name, home address and passport number for natural persons; (b) company name, address and list of persons having access to the terminal equipment with their names, patronymics and family names, home addresses and passport numbers for legal persons; (c) information about connections, traffic and payments (paragraph 14).

### (d) Order no. 6

134. Order no. 6 on requirements for telecommunications networks concerning the conduct of operational-search activities, Part I, issued by the Ministry of Communications on 16 January 2008, replaced Order no. 130.

135. It retained the requirement that communications service providers had to ensure transmittal to the relevant law-enforcement agency's remote-control terminal of information about (a) subscribers' numbers and identification codes; and (b) the contents of their communications. The information must be transmitted in real time following a request from the remote-control terminal. Communications service providers must also ensure that the subscriber's location is identified (paragraphs 2, 3 and 5).

136. The remote-control terminal must have access to databases containing information about subscribers, including their numbers and identification codes (paragraphs 7 and 8).

137. Communications service providers must ensure that the interception subject remains unaware of the interception of his communications. Information about ongoing or past interceptions must be protected from unauthorised access by the employees of the communications service providers (paragraph 9).

### (e) Order no. 73

138. Order no. 73 on requirements for telecommunications networks concerning the conduct of operational-search activities, Part II, issued by the Ministry of Communications on 27 May 2010, elaborates on certain requirements contained in Order no. 6. In particular, it provides that the equipment installed by communications service providers must ensure that agencies performing operational-search activities have access to all data transmitted through the telecommunications networks and are capable of selecting data and transmitting the selected data to its control terminal (paragraph 2).

## III. RELEVANT INTERNATIONAL AND EUROPEAN INSTRUMENTS

### A. United Nations

139. Resolution no. 68/167, on The Right to Privacy in the Digital Age, adopted by the General Assembly on 18 December 2013, reads as follows:

> "The General Assembly,
>
> . . .
>
> 4. *Calls upon* all States:
>
> . . .
>
> (*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;
>
> (*d*) 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 . . ."

### B. Council of Europe

140. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (CETS No. 108, hereafter "Convention no. 108") sets out standards for data protection in the sphere of automatic processing of personal data in the public and private sectors. It reads:

> **"Article 8 – Additional safeguards for the data subject**
>
> Any person shall be enabled:

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

**Article 9 – Exceptions and restrictions**

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others . . .

**Article 10 – Sanctions and remedies**

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

141. Convention no. 108 was ratified by Russia on 15 May 2013 and entered into force in respect of Russia on 1 September 2013. The instrument of ratification deposited by the Russian Federation on 15 May 2013 contains the following declaration:

"The Russian Federation declares that in accordance with subparagraph "a" of paragraph 2 of Article 3 of the Convention, it will not apply the Convention to personal data:

. . .

(b) falling under State secrecy in accordance with the legislation of the Russian Federation on State secrecy.

The Russian Federation declares that in accordance with subparagraph "c" of paragraph 2 of Article 3 of the Convention, it will apply the Convention to personal data which is not processed automatically, if the application of the Convention corresponds to the nature of the actions performed with the personal data without using automatic means.

The Russian Federation declares that in accordance with subparagraph "a" of paragraph 2 of Article 9 of the Convention, it retains the right to limit the right of the data subject to access personal data on himself for the purposes of protecting State security and public order."

142. The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181), signed but not ratified by Russia, provides as follows:

**"Article 1 – Supervisory authorities**

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts . . ."

143. A Recommendation by the Committee of Ministers, regulating the use of personal data in the police sector, adopted on 17 September 1987 (No. R (87) 15), reads as follows:

"1.1. Each member state should have an independent supervisory authority outside the police sector which should be responsible for ensuring respect for the principles contained in this recommendation . . .

2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

2.2. Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced . . .

3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law . . .

5.2.i. Communication of data to other public bodies should only be permissible if, in a particular case:

a. there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority, or if

b. these data are indispensable to the recipient to enable him to fulfil his own lawful task and provided that the aim of the collection or processing to be carried out by the recipient is not incompatible with the original processing, and the legal obligations of the communicating body are not contrary to this.

5.2.ii. Furthermore, communication to other public bodies is exceptionally permissible if, in a particular case:

a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if

b. the communication is necessary so as to prevent a serious and imminent danger.

5.3.i. The communication of data to private parties should only be permissible if, in a particular case, there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority . . .

6.4. Exercise of the rights [of the data subject] of access, rectification and erasure should only be restricted insofar as a restriction is indispensable for the performance of a legal task of the police or is necessary for the protection of the data subject or the rights and freedoms of others . . .

6.5. A refusal or a restriction of those rights should be reasoned in writing. It should only be possible to refuse to communicate the reasons insofar as this is indispensable for the performance of a legal task of the police or is necessary for the protection of the rights and freedoms of others.

6.6. Where access is refused, the data subject should be able to appeal to the supervisory authority or to another independent body which shall satisfy itself that the refusal is well founded.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored.

For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject, particular categories of data.

7.2. Rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law.

8. The responsible body should take all the necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration. The different characteristics and contents of files should, for this purpose, be taken into account."

144. A Recommendation by the Committee of Ministers on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, adopted on 7 February 1995 (No. R (95) 4), reads in so far as relevant as follows:

"2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:

a. the exercise of the data subject's rights of access and rectification;

b. in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;

c. storage or destruction of such data.

If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference . . . "

### C. European Union

145. Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01) provides as follows:

"This section presents the requirements of law enforcement agencies relating to the lawful interception of telecommunications. These requirements are subject to national law and should be interpreted in accordance with applicable national policies . . .

1.3. Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization . . .

2. Law enforcement agencies require a real-time, fulltime monitoring capability for the interception of telecommunications. Call associated data should also be provided in real time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.

3. Law enforcement agencies require network operators/service providers to provide one or several interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

> and the network operators/service providers. Other issues associated with these interfaces will be handled according to accepted practices in individual countries . . .
>
> 5. Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception . . .
>
> 5.2. Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization . . ."

146. The above requirements were confirmed and expounded in Council Resolution No. 9194/01 of 20 June 2001 on law-enforcement operational needs with respect to public telecommunication networks and services.

147. The judgment adopted by the Court of Justice of the European Union (the CJEU) on 8 April 2014 in the joint cases of *Digital Rights Ireland* and *Seitinger and Others* declared invalid the Data Retention Directive 2006/24/EC laying down the obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years, in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The CJEU noted that, even though the directive did not permit the retention of the content of the communication, the traffic and location data covered by it might allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained. Accordingly, the obligation to retain those data constituted in itself an interference with the right to respect for private life and communications guaranteed by Article 7 of the Charter of Fundamental Rights of the EU and the right to protection of personal data under Article 8 of the Charter. Furthermore, the access of the competent national authorities to the data constituted a further interference with those fundamental rights. The CJEU further held that the interference was particularly serious. The fact that data were retained and subsequently used without the subscriber or registered user being informed was likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance. The interference satisfied an objective of general interest, namely to contribute to the fight against serious crime and terrorism and thus, ultimately, to public security. However, it failed to satisfy the requirement of proportionality. Firstly, the directive covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. It therefore entailed an interference with the fundamental rights of practically the entire European population. It applied even to persons for whom there was no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Secondly, the directive did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. By simply referring, in a general manner, to serious crime, as defined by each Member State in its national law, the directive failed to lay down any objective criterion by which to determine which offences might be considered to be sufficiently serious to justify such an extensive interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued. Thirdly, the directive required that all data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, without such an interference being precisely circumscribed by provisions to ensure that it was actually limited to what was strictly necessary. The CJEU also noted that the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

## 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

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

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

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

#### B. Merits

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

###### (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 contravened 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;

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

*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 (see paragraph 128 above). 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*

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

*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, §§ 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. (see paragraph 128 above), 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 (see paragraph 8 above). 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, § 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*

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

*GmbH & Co. KG v. Austria (no. 4)*, no. 72331/01, § 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 particular 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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

*(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 (see paragraph 58 above).

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 (see paragraph 31 above). 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 (see paragraph 48 above). 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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 (see paragraph 42 above), 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 (see paragraph 41 above), 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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 (see paragraph 40 above)

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

*(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 (see paragraph 83 above).

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 general jurisdiction in accordance with the procedure established by Chapter 25 of the Code of Civil Procedure (see paragraph 92 above). 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 (see paragraph 97 above). 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 (see paragraph 43 above). 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 (see paragraph 102 above). 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 (see paragraphs 103 and 104 above). 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) (see paragraphs 19 to 22 above). 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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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, § 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;

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

(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 (see paragraph 26 above). 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 (see paragraph 128 above).

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 (see paragraphs 115 to 122 above), 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* (see paragraph 115 above). 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).

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 (see paragraphs 31 to 33 above). 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 (see paragraph 32 above). 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 (see paragraph 31 above). 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.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

*(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 authorities 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 (see paragraphs 38 and 47 above). 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 (see paragraphs 51 to 57 above). 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 (see paragraphs 58 to 64 above). 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 (see paragraphs 65 and 66 above).

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 (see paragraph 66 above). 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 independent 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 (see paragraphs 34 and 44 above). 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 (see paragraphs 37 and 46 above). The judge must give reasons for the decision to authorise interceptions (see paragraphs 38 and 44 above).

260. Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means (see *Klass and Others,* cited above, § 51; *Association for European Integration and Human Rights and Ekimdzhiev,* cited above, §§ 79 and 80; *Iordachi and Others*, cited above, § 51; and *Kennedy,* cited above, §§ 31 and 32).

261. The Court notes that in Russia judicial scrutiny is limited in scope. Thus, materials containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures may not be submitted to the judge and are therefore excluded from the court's scope of review (see paragraph 37 above). The Court considers that the failure to disclose the relevant information to the courts deprives them of the power to assess whether there is a sufficient factual basis to suspect the person in respect of whom operational-search measures are requested of a criminal offence or of activities endangering national, military, economic or ecological security (see, *mutatis mutandis*, *Liu,* cited above, §§ 59-63). The Court has earlier found that there are techniques that can be employed which both accommodate legitimate security concerns about the nature and sources of intelligence information and yet accord the individual a substantial measure of procedural justice (see, *mutatis mutandis*, *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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

if he or she is persuaded that interception is lawful, necessary and justified. The Constitutional Court has also held that the judicial decision authorising interception should contain reasons and refer to specific grounds for suspecting that a criminal offence has been committed, or is ongoing, or is being plotted or that activities endangering national, military, economic or ecological security are being carried out, as well as that the person in respect of whom interception is requested is involved in these criminal or otherwise dangerous activities (see paragraphs 40 to 42 above). The Constitutional Court has therefore recommended, in substance, that when examining interception authorisation requests Russian courts should verify the existence of a reasonable suspicion against the person concerned and should authorise interception only if it meets the requirements of necessity and proportionality.

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

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

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

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 (see paragraph 35 above). 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 (see paragraph 48 above). 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 (see paragraphs 115 to 122 above). 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 (see paragraphs 132 and 133 above). 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. Although 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 (see paragraph 120 above). The Court has

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 (see paragraphs 69 to 80 above). 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 insufficiently independent (see *Iordachi and Others,* cited above, § 47).

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

280. Furthermore, it is essential that any role prosecutors have in the general protection of human rights does not give rise to any conflict of interest (see *Menchinskaya v. Russia*, no. 42454/02, §§ 19 and 38, 15 January 2009). The Court observes that prosecutor's offices do not specialise in supervision of interceptions (see paragraph 71 above). Such supervision is only one part of their broad and diversified functions, which include prosecution and supervision of criminal investigations. In the framework of their prosecuting functions, prosecutors give their approval to all interception requests lodged by investigators in the framework of criminal proceedings (see paragraph 44 above). This blending of functions within one 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 (see paragraph 74 above). The scope of their supervision is therefore limited. Moreover, interceptions performed by the FSB in the sphere of counterintelligence may be inspected only following an individual complaint (see paragraph 76 above). As individuals are not notified of interceptions (see paragraph 81 above and paragraph 289 below), it is unlikely that such a complaint will ever be lodged. As a result, surveillance measures related to counter-intelligence *de facto* escape supervision by prosecutors.

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

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 (see paragraph 80 above). It follows that in Russia supervision by prosecutors is conducted in a manner which is not open to public scrutiny and knowledge.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

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

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

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, see paragraph 143 above).

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 (see paragraph 81 above). 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 (see paragraph 52 above). 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 (see paragraph 83 above). The Court reiterates that a hierarchical appeal to a direct supervisor of the authority whose actions are being challenged does not meet the requisite standards of independence needed to constitute sufficient protection against the abuse of authority (see, for similar reasoning, *Khan v. the United Kingdom*, no. 35394/97, §§ 45-47, ECHR 2000-V; *Dumitru Popescu (no. 2),* cited above, § 72; and *Avanesyan,* cited above, § 32). A prosecutor also lacks independence and has a limited scope of review, as demonstrated above (see paragraphs 277 to 285 above). It remains to be ascertained whether a complaint to a court may be regarded as an effective remedy.

293. There are four judicial procedures which, according to the Government, may be used by a person wishing to complain about interception of his communications: an appeal, a cassation appeal or a supervisory-review complaint against the judicial decision authorising interception of communications; a judicial review complaint under Article 125 of the CCrP; a judicial review complaint under the Judicial Review Act and Chapter 25 of the Code of Civil Procedure; and a civil tort claim under Article 1069 of the Civil Code. The Court will examine them in turn.

294. The first of the procedures invoked by the Government is an appeal, cassation appeal or supervisory-review complaint against the judicial decision authorising interception of communications. However, the Constitutional Court stated clearly that the interception subject had no right to appeal against the judicial decision authorising interception of his communications (see paragraph 40 above; see also *Avanesyan*, cited above, § 30). Domestic law is silent on the possibility of lodging a cassation appeal. Given that the Government did not submit any examples of domestic practice on examination of cassation appeals, the Court has strong doubts as to the existence of a right to lodge a cassation appeal against a judicial decision authorising interception of communications. At the same time, the interception subject is clearly entitled to lodge a supervisory review complaint (see paragraph 43 above). However, in order to lodge a supervisory review complaint against the judicial decision authorising interception of communications, the person concerned must be aware that such a decision exists. Although the Constitutional Court

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 (see paragraphs 88 and 89 above). 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 (see paragraphs 85, 95, 96 and 105 above). In the absence of notification or some form of access to official documents relating to the interceptions such a burden of proof is virtually impossible to satisfy. Indeed, the applicant's judicial complaint was rejected by the domestic courts on the ground that he had failed to prove that his telephone communications had been intercepted (see paragraphs 11 and 13 above). The Court notes that the Government submitted several judicial decisions taken under Chapter 25 of the Code of Civil Procedure or Article 1069 of the Civil Code (see paragraphs 220 to 223 above). However, all of those decisions, with one exception, concern searches or seizures of documents or objects, that is, operational-search measures carried out with the knowledge of the person concerned. Only one judicial decision concerns interception of communications. In that case the intercept subject was able to discharge the burden of proof because she had learned about the interception of her communications in the course of criminal proceedings against her.

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

298. The Court concludes from the above that the remedies referred to by the Government are available only to persons who are in possession of information about the interception of their communications. Their effectiveness is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. Accordingly, the Court finds that Russian law does not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject. 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 (see paragraphs 40 to 43, 50, 82 and 85 to 87 above). In such circumstances the Court finds it unlikely that a complaint by the applicant to the

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

Constitutional Court, raising the same issues that have already been examined by it, would have any prospects of success. Nor is the Court convinced that a challenge of Order no. 70 before the Supreme Court or the lower courts would constitute an effective remedy. Indeed, the applicant did challenge Order no. 70 in the domestic proceedings. However, both the District and City Courts found that the applicant had no standing to challenge the Order because the equipment installed pursuant to that order did not in itself interfere with the privacy of his communications (see paragraphs 10, 11 and 13 above). It is also significant that the Supreme Court found that Order no. 70 was technical rather than legal in nature (see paragraph 128 above).

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

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

*(θ) Conclusion*

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

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

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

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

## 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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

308. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

### A. Damage

309. The applicant claimed 9,000 euros (EUR) in respect of non-pecuniary damage.

310. The Government submitted that the claim was excessive, taking into account that the applicant had challenged Russian law *in abstracto* without being in any way personally affected by it. The finding of a violation would therefore constitute sufficient just satisfaction.

311. The Court reiterates that, in the context of the execution of judgments in accordance with Article 46 of the Convention, a judgment in which it finds a violation of the Convention or its Protocols imposes on the respondent State a legal obligation not just to pay those concerned any sums awarded by way of just satisfaction, but also to choose, subject to supervision by the Committee of Ministers, the general and/or, if appropriate, individual measures to be adopted in its domestic legal order to put an end to the violation found by the Court and make all feasible reparation for its consequences in such a way as to restore as far as possible the situation existing before the breach. Furthermore, in ratifying the Convention, the Contracting States undertake to ensure that their domestic law is compatible with it (see *Association for European Integration and Human Rights and Ekimdzhiev,* cited above, § 111, with further references).

312. The Court considers that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage caused to the applicant.

### B. Costs and expenses

313. Before the Chamber, the applicant claimed 26,579 Russian roubles (RUB, about 670 euros (EUR) on the date of submission) for postal and translation expenses. He relied on postal and fax service invoices and a translation services contract.

314. Before the Grand Chamber, the applicant claimed 22,800 pounds sterling (GBP, about EUR 29,000 on the date of submission) and EUR 13,800 for legal fees. He relied on lawyers' time-sheets. Relying on bills and invoices, he also claimed GBP 6,833.24 (about EUR 8,700 on the date of submission) for translation, travelling and other administrative expenses.

315. The Government accepted the claim for costs and expenses made before the Chamber because it was supported by documentary evidence. As regards the claims for costs and expenses made before the Grand Chamber, the Government submitted that the claims had been submitted more than a month after the hearing. As regards the legal fees, the Government submitted that part of those fees covered the work performed by the representatives before the applicant had signed an authority form and that there was no authority form in the name of Ms Levine. Furthermore, the number of representatives and the number of hours spent by them on the preparation of the case had been excessive. There was moreover no evidence that the applicant had paid the legal fees in question or was under a legal or contractual obligation to pay them. As regards the translation and other administrative expenses, the Government submitted that the applicant had not submitted any documents showing that he had paid the amounts claimed. Nor had he proved that the translation expenses had been indeed necessary, given that some of the applicant's lawyers spoke Russian. The rates claimed by the translators had been excessive. Lastly, the travelling expenses had been also excessive.

316. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 40,000 covering costs under all heads, plus any tax that may be chargeable to the applicant.

### C. Default interest

317. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT

1. *Joins*, unanimously, to the merits the Government's objections regarding the applicant's lack of victim status and non-exhaustion of domestic remedies and *declares* the application admissible;
2. *Holds*, unanimously, that there has been a violation of Article 8 of the Convention and *dismisses* the Government's above-mentioned objections;
3. *Holds*, unanimously, that there is no need to examine the complaint under Article 13 of the Convention;
4. *Holds*, by sixteen votes to one, that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant;
5. *Holds*, unanimously,

   (a) that the respondent State is to pay the applicant, within three months, EUR 40,000 (forty thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;

   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;
6. *Dismisses*, unanimously, the remainder of the applicant's claim for just satisfaction.

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

Lawrence Early
Jurisconsult

Dean Spielmann
President

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

(a) Concurring opinion of Judge Dedov;

(b) Partly dissenting opinion of Judge Ziemele.

D.S.

T.L.E.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

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 interconnection 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".

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press

## 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.

https://doi.org/10.5305/intelegamate.55.2.0207 Published online by Cambridge University Press