

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

FIFTH SECTION

CASE OF THE ASSOCIATION FOR EUROPEAN INTEGRATION AND HUMAN RIGHTS AND EKIMDZHIEV v. BULGARIA

(Application no. 62540/00)

JUDGMENT

STRASBOURG

28 June 2007

<u>FINAL</u>

30/01/2008

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

1

In the case of the Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,

The European Court of Human Rights (Fifth Section), sitting as a Chamber composed of:

Mr P. LORENZEN, President,

Mrs S. Botoucharova,

Mr K. JUNGWIERT,

Mr V. BUTKEVYCH,

Mrs M. TSATSA-NIKOLOVSKA,

Mr R. MARUSTE,

Mr M. VILLIGER, judges,

and Mrs C. WESTERDIEK, Section Registrar,

Having deliberated in private on 5 June 2007,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

- 1. The case originated in an application (no. 62540/00) against the Republic of Bulgaria lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") on 13 September 2000. It was lodged by the Association for European Integration and Human Rights, a non-profit association founded in March 1998 and having its registered office in Plovdiv ("the applicant association") and by Mr Mihail Ekimdzhiev, a Bulgarian national who was born in 1964 and lives in Plovdiv ("the second applicant").
- 2. The applicant association was represented by the second applicant, who is a lawyer and who acted *pro se*. The Bulgarian Government ("the Government") were represented by their Agent, Ms M. Kotseva, of the Ministry of Justice.
- 3. The applicants alleged that the Bulgarian legislation allowing the use of secret surveillance measures infringed their rights under Articles 6 § 1, 8 and 13 of the Convention, as it fell short of the standards stemming from the Court's case-law under these provisions.
- 4. On 10 June 2005 the Court decided to give notice of the application to the Government. Under the provisions of Article 29 § 3 of the Convention, it decided to examine the merits of the application at the same time as its admissibility.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

- 5. One of the principal aims of the applicant association is the protection of human rights. The second applicant is a lawyer. His practice includes acting as counsel in civil and criminal cases in the courts in Plovdiv and representing applicants in proceedings before the European Court of Human Rights.
- 6. Their application is directed against the Special Surveillance Means Act of 1997, a piece of legislation which presently regulates the use of special means of surveillance in Bulgaria. The applicants do not aver that surveillance measures have in fact been ordered or implemented against them, nor that they have been indirectly involved in a surveillance measure directed against other persons. They contend that under the law as it stands they may be subjected to such measures at any point in time without any notification prior to, during, or after the said measures are applied.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The Constitution of 1991

7. The relevant provisions of the Constitution of 1991 are:

Article 32

- "1. The private life of citizens shall be inviolable. Everyone shall have the right to be protected against unlawful interferences with his private and family life and against encroachments on his honour, dignity and reputation.
- 2. No one may be spied on, photographed, filmed, recorded, or subjected to similar actions without his or her knowledge or despite his or her express disagreement, except in cases provided for by law."

Article 33 § 1

"The home shall be inviolable. No one may enter or remain in it without the consent of its inhabitant, except in the cases expressly specified by law."

Article 34

"1. The freedom and secret of correspondence and other communications shall be inviolable.

2. This rule may be subject to exceptions only with the permission of the judicial authorities when necessary for uncovering or preventing serious offences."

Article 41 § 2

"Citizens shall have the right to information from state bodies or agencies on any matter of legitimate interest to them, unless the information is a state secret or a secret protected by law, or affects the rights of others."

Article 117 § 2

"The judiciary shall be independent. In carrying out their duties the judges, the jurors, the prosecutors and the investigators shall have regard solely to the law."

B. The Special Surveillance Means Act of 1997

- 8. The Special Surveillance Means Act of 1997 ("Закон за специалните разузнавателни средства" "the SSMA"), which presently is the principal legislative enactment regulating the use of special means of surveillance, was adopted in October 1997. It underwent minor amendments in August 1999 and June 2000, more extensive ones in February 2003, and some further minor changes in April 2006. Its essential provisions have however remained intact since its adoption and the account which follows is based on their present version.
- 9. The SSMA governs the conditions for and the manner of use of special means of surveillance, as well as the control of their use and of the results obtained thereby (section 1(1)). It defines special means of surveillance as technical devices which can be used for creating photographs, audio and video recordings and marked objects, as well as the methods for operating them (section 2(1)).
- 10. By section 3(1) of the SSMA, special means of surveillance may be used when necessary to prevent or uncover serious offences (Article 93 § 7 of the Criminal Code of 1968 defines a "serious" offence as one punishable by more than five years' imprisonment), if the requisite intelligence cannot be obtained through other means. Section 4 provides that special means of surveillance may also be used for activities relating to national security.
- 11. Special means of surveillance may be used against persons suspected, on the basis of the information available, of planning, committing, or having committed serious offences, or against persons who might be unwittingly involved in the above by the suspected perpetrators. Such means may also be used against persons and objects related with national security (section 12(1)). Such means may also be used in respect of persons who have agreed to that in writing, to protect their lives or property (section 12(2)).

- 12. Only the following bodies may request the use of special means of surveillance and draw on the intelligence obtained thereby, in the spheres of their respective competencies: (i) the central "Security" and "Police" services of the Ministry of Internal Affairs, as well as the national and territorial directorates of that Ministry; (ii) the "Military Information" and "Military Police and Military Counter-Intelligence" services of the Ministry of Defence; (iii) the National Intelligence Service; (iv) the National Investigation Service, the Sofia Investigation Service and the regional investigation services; (v) the Prosecutor-General, the Supreme Cassation Prosecutor's Office, the Supreme Administrative Prosecutor's Office, the Military Appellate Prosecutor's Office, the appellate prosecutor's offices, the Sofia City Prosecutor's Office and the regional and regional-military prosecutor's offices (section 13(1) and (2)).
- 13. The procedure for deploying special means of surveillance starts with a written application by the head of the respective service. The application must set out in detail the circumstances grounding the suspicion that a serious offence is being planned or committed or has been committed, so as to justify the use of surveillance. It must also fully describe the steps which have already been undertaken and the results of the hitherto inquiries or investigations. It has to contain information allowing the identification of the persons or objects to be subjected to surveillance, its duration, and the methods to be used. Finally, the application has to specify the name of the official to be informed of the results obtained (section 14(1)).
- 14. The application is made to the president of the Sofia City Court or of the respective regional court, or to a duly authorised deputy (for military personnel the application is made to the president of the deputy-president of the respective military regional court) who may issue a warrant (section 15(1)). If they refuse to issue a warrant, the application may be re-submitted to the president or a duly authorised deputy of the respective court of appeals (section 15(3)). The decision whether or not to issue a warrant must be taken immediately upon receipt of the application, and the originals of the application and of the warrant must be returned to the service which has made the application (section 15(2)).
- 15. After the warrant is issued, the Minister of Internal Affairs or a deputy-minister designated in writing by the Minister makes a written order for the deployment of special means of surveillance (section 16). In urgent cases, this step of the procedure may be skipped and the deployment may start immediately upon the issue of the warrant (section 17). However, in that case the Minister or the deputy-minister must be informed without delay (ibid.).
- 16. Section 18(1) of the SSMA provides for an exception to the procedure outlined above in cases where there is an immediate risk that a serious intentional offence may be committed or where there is an immediate threat to national security. In such cases, the Minister of Internal

Affairs or a deputy-minister designated by the Minister may order the deployment of special means of surveillance without a judicial warrant. The deployment of these means must be discontinued if the warrant is not issued within twenty-four hours (section 18(2)). In that case, the president or the vice-president of the respective court decides whether the material obtained is to be kept or destroyed (ibid.). He or she may thus retrospectively validate the use of special means of surveillance (section 18(3)).

- 17. The Minister of Internal Affairs or a deputy-minister authorised in writing may discontinue the use of special means of surveillance at any time before the planned end of the surveillance. In that case, the president or the vice-president of the respective court must be informed in writing (section 19).
- 18. The only services which are authorised to deploy special means of surveillance are the "Operative and Technical Information", the "Operative Tracking" and the "Protection of the Means of Communication" directorates of the Ministry of Internal Affairs (section 20(1)). However, the National Intelligence Service and the intelligence services of the Ministry of Defence may also deploy such means in the performance of their duties (section 20(2)).
- 19. Special means of surveillance may be used for a maximum of two months (section 21(1)). This time may, if necessary, be extended by the president or the vice-president of the respective court for up to six months, by a fresh warrant (section 21(2)).
- 20. The use of special means of surveillance must be discontinued after the expiry of the time-limit set in the warrant, after the desired aims have been attained, or if the use of the means proves fruitless (section 22(1)).
- 21. The intelligence obtained by such means must be recorded (section 24). It must then, immediately after being obtained, be put down in writing by the service which has in fact deployed the means (section 25(1)). The resulting document, which must faithfully reflect the contents of the recordings, is sent to the body which has requested the use of such means, possibly along with photographs and recordings (section 25(2), (3) and (4)). While the special means of surveillance are still being used, the original recordings must be kept at the service which has deployed them (section 25(5)).
- 22. If at the end of the period of authorised surveillance the sought intelligence has been obtained, the service which has deployed the means of surveillance draws up a note of physical evidence (section 27). The same is done if the sought intelligence has been obtained before the end of the period, pursuant to the written request of the body which has requested the measures (section 26). Conversely, if the use of the means is fruitless, the body which has requested it advises in writing the service which deploys them that their use is to be discontinued. In that case no note of physical

evidence is drawn up and the material obtained is destroyed (section 28(1) and (2)).

- 23. The note of physical evidence must conform to the requirements of the Code of Criminal Procedure (section 29(1)). It has to be signed by the head of the service which has deployed the means (section 29(2)) and refer to the application for their use, the order of the Minister or the deputy-minister and the judicial warrant (section 29(3)). It has to specify the time and place of the use of the means, the types of devices and methods employed, the intelligence obtained, the textual reproduction of this intelligence, and the physical conditions under which the intelligence has been acquired (section 29(4)). The raw data is part of the record (section 29(5)). The evidence thus obtained is kept by the Ministry of Internal Affairs pending the opening of a criminal investigation. After the opening of an investigation the evidence is kept by the respective judicial authorities (section 31(1) and (2)). The intelligence which is not used as evidence has to be destroyed by the directorate which has deployed the means within ten days and the destruction has to be recorded in minutes (section 31(3)).
- 24. If the special means of surveillance have yielded results outside the scope of the initial application for their use and if these results come within the purview of other bodies allowed to request the use of such means (see paragraph 12 above), the Minister of Internal Affairs or the duly authorised deputy-minister must be notified immediately. He or she then decides how this intelligence is to be used (section 30).
- 25. The information obtained by using special means of surveillance may not be used for ends other than the prevention and detection of offences, or the gathering of evidence for the perpetration of offences, in accordance with the conditions and the manner specified by the law (section 32).
- 26. All persons who come across information about the use of special means of surveillance under the conditions and according to the manner set out in the SSMA, or intelligence obtained thereby, are under a duty not to disclose it (section 33).
- 27. The overall control over the use of special means of surveillance and the intelligence obtained thereby is entrusted to the Minister of Internal Affairs, who may issue instructions for the application of the SSMA (section 34(1) and paragraph 2 of the concluding provisions of the Act). The directorates which deploy these means may also carry out inspections to check whether special means of surveillance have been unlawfully used (section 34(2)).
- 28. To date, no instructions or regulations on the implementation of the SSMA have been published in the State Gazette.

C. The Constitutional Court's judgment in case no. 17/1997

- 29. In a judgment of 10 February 1998, published in the State Gazette on 17 February 1998 (реш. № 1 от 10 февруари 1998 г. по конституционно дело № 17 от 1997 г., обн., ДВ, бр. 19 от 17 февруари 1998 г.) the Constitutional Court rejected an application by the Prosecutor-General to declare sections 18(1), 19, 30 and 34(1) of the SSMA contrary to Articles 34 § 2 and 117 § 1 of the Constitution.
- 30. The court started by noting that the special means of surveillance regulated by the SSMA amounted to interferences with private life, home and correspondence, all of which were permissible under Articles 32 § 2, 33 and 34 § 2 of the Constitution (see paragraph 7 above).
- 31. The court then proceeded to examine section 18(1) of the SSMA, which allows, under certain conditions, the use of special means of surveillance before the issue of judicial warrant. It held that Article 34 § 2 of the Constitution could not be read as requiring the prior issue of warrant in every case. The risk of abuse by the executive was reduced by the facts that the possibility of dispensing with prior judicial control was narrowly circumscribed and that immediate subsequent control was mandatory. This state of affairs was also compatible with Article 8 of the Convention and Article 17 of the International Covenant on Civil and Political Rights. In the court's view, the SSMA provided an even higher level of protection than these instruments.
- 32. As regards section 19 of the SSMA, the court found that the possibility for the Minister of Internal Affairs to discontinue the use of special means of surveillance was not violative of Article 117 § 2 of the Constitution. While by Article 34 § 2 of the Constitution and section 15 of the SSMA the judiciary alone was empowered to authorise the use of such means, it was not the only branch of government which could order the termination of their use. The prerogative of the Minister did not therefore impinge on the independence of the judiciary.
- 33. With regard to section 30 of the SSMA, the court held that its true meaning, when read in the context of the Act as a whole, was not that the Minister of Internal Affairs could order the use of special means of surveillance anew if intelligence outside the scope of the initial request for their use was obtained. It was rather to be construed as allowing the Minister to decide to which authority to forward the intelligence already obtained. His powers in this respect were thus not in breach of Article 117 § 2 of the Constitution.
- 34. Concerning section 34(1) of the SSMA, which entrusts the overall control over the system to the Minister of Internal Affairs, the court noted that it was impossible to empower another minister, let alone a non-executive body, with such functions, because that would disrupt the equality between, and the independence of, the three branches of

government. This followed also from paragraph 2 of the concluding provisions of the SSMA, which allowed the Minister to issue instructions for its application. Moreover, the logic of the system, which was apparent from the wording of section 31 of the Act, required that the Minister be made responsible for controlling the use of the special means of surveillance until the moment when the intelligence obtained thereby was given to the judicial authorities. Therefore, the judicial control over the intelligence thus gathered had not been infringed and the resulting situation was compatible with Article 117 § 2 of the Constitution.

- 35. Two judges dissented in part.
- 36. One of them was of the opinion that section 34(1) of the SSMA, which entrusts the control over the use of special means of surveillance to the Minister of Internal Affairs, was unconstitutional. In his view, this provision was not sufficiently precise and the powers it conferred to the Minster were not clearly delineated. It followed from the reading of the SSMA as a whole that the Minister had powers in respect of both the use and the control over the use of special means of surveillance, which was inadmissible. The resulting lack of external control meant that section 34(1) was unconstitutional. When the law spoke about control over the system, it meant control over both its functioning as a whole and control in specific cases. To bestow controlling functions to the Minister, who also played a key part in the operation of the system, did not provide sufficient safeguards against the unwarranted use of special means of surveillance.
- 37. The other dissenting judge considered that section 18(1) of the SSMA was unconstitutional, in that it allowed the Minister of Internal Affairs to order the use of special means of surveillance without the prior issue of judicial warrant, even in cases when their use would interfere with the freedom of correspondence or other communications. In his view, Article 34 § 2 of the Constitution, which protects those freedoms, required prior judicial authorisation in all cases.

D. The Codes of Criminal Procedure of 1974 and 2005

- 38. Articles 111-13a of Code of Criminal Procedure of 1974 ("the Code of 1974") also regulated the use of special means of surveillance in the context of pending or impending criminal proceedings. They coincided almost verbatim with the provisions of the SSMA. One difference was that Article 111b § 6 provided that the judge who issued the warrant had to be informed in writing when the use of the means was discontinued. If their use had been fruitless, he or she was to order the destruction of the material obtained.
- 39. These provisions were superseded by Articles 172-77 of the Code of Criminal Procedure of 2005 ("the Code of 2005"), which entered into force on 29 April 2006.

- 40. By Article 172 §§ 1 and 2 of the Code of 2005, the investigation authorities may use special means of surveillance for investigating certain serious offences, which are exhaustively listed, if the relevant facts cannot be established in another manner or if their establishment would be extremely difficult. Such means may be used for a maximum duration of two months (Article 175 § 3), which may, if needed, be extended by four months (Article 175 § 4).
- 41. The procedure starts with a reasoned application made by the prosecutor in charge of the case (Article 173 § 1). The application must contain information about the offence under investigation, a description of the hitherto investigative steps and their results, information about the persons or objects which will be subjected to surveillance, the methods which will be used and the duration of the surveillance (Article 173 § 2). The surveillance warrant is issued under the hand of the president of the respective regional court or of a specifically authorised deputy (Article 174) § 1). He or she must issue the warrant or refuse to do so immediately after receiving the application, and give reasons (Article 174 § 3). If he or she refuses, the application may be re-submitted to the president of the respective court of appeals or a specifically authorised deputy (Article 174 § 4). All applications and warrants are recorded in a special non-public register (Article 174 § 6). The Code of 2005 makes no provision for exceptions from this procedure save in the case of an undercover agent, who may, in urgent cases, start to operate pursuant to a prosecutor's order, which must be confirmed by the respective judge within twenty-four hours (Article 173 § 4).
- 42. After the issue of warrant the special means of surveillance are deployed in accordance with the provisions of the SSMA (Article 175 § 1). The judge who issued the warrant must be informed in writing when the use of the means is discontinued. If their use has been fruitless, the judge orders the destruction of the material obtained (Article 175 § 6).

E. Relevant provisions of the Protection of Classified Information Act of 2002

- 43. The Protection of Classified Information Act of 2002 ("Закон за защита на класифицираната информация" "the PCIA"), which was enacted in April 2002 and amended several times thereafter, provides a comprehensive framework for the creation, processing and storage of classified information, as well as the conditions and the procedure for providing access to such information (section 1(1)). "Classified information" includes information which is a state or an official secret (section 1(3)).
- 44. Section 25 defines a "state secret" as the "information set out in Schedule No. 1 [to the Act], the unregulated access to which could endanger

or prejudice the interests of the Republic of Bulgaria and which relates to the national security, the defence, the foreign policy, or the protection of the constitutional order". Schedule No. 1 to the Act sets out a list of the categories of information which are liable to be classified as being a state secret. Thus, the information about special means of surveillance (technical devices and/or the manner of their use) used pursuant to the law is a state secret (point 6 of part II of Schedule No. 1). So is the intelligence obtained as a result of the use of such means (point 8 of part II of Schedule No. 1).

- 45. Section 26(1) defines an "official secret" as the "information created or stored by state or local government authorities, which is not a state secret, but the unregulated access to which could have a negative impact on the interests of the State or on another legally protected interest". By section 26(2), the information classified as an "official secret" must be set out in a statute.
- 46. Section 34(1) lays down time-limits for protecting classified information. They vary from thirty years for information marked as "highly secret" to two years for information graded as an "official secret". These time-limits may be extended, but by not more than the double of their original length (section 34(2)). After the expiration of these time-limits the access to this information is effected in accordance with the Access to Public Information Act of 2000 (section 34(3)).
- 47. While the information is classified, it may be accessed only under certain conditions and by limited categories of persons, which must, in most cases, undergo a security check and obtain a security clearance (sections 36-71).
- 48. Section 33(3) provides that classified information may not be destroyed earlier than one year after the expiration of the time-limit for its protection. The destruction of such information is possible only by virtue of a decision of the State Information Security Commission, made pursuant to the proposal of a special commission (section 33(4)). The Commission's decision is subject to review by the Supreme Administrative Court (section 34(5)).

F. The judgment of the Supreme Administrative Court in case no. 9881/2003

49. In a final judgment of 12 February 2004 (реш. № 1195 от 12 февруари 2004 г. по адм. д. № 9881/2003 г.), given pursuant to an appeal by a person who had been refused information on whether the use of special means of surveillance had been authorised against him during the period 1 January 1996 – 1 November 2001, the Supreme Administrative Court held that while Article 41 of the Constitution enshrined the right to obtain information from a state body, that right was subject to limitations when, for instance, this information was a state or an official secret. It was

apparent from section 33 of the SSMA that information about the use of special means of surveillance was not to be disclosed. The refusal to provide the requested information was thus compatible with Article 32 § 2 of the Constitution and Article 8 of the Convention. The appellant's argument that the refusal had been in breach of the Protection of the Personal Data Act of 2002 was inapposite, because the material gathered pursuant to the SSMA was outside the purview of the Protection of the Personal Data Act of 2002, as was the information whether the use of special means of surveillance had been authorised. The appellant's further arguments that the information requested was not a state or an official secret within the meaning of sections 25 and 26 of the PCIA and could moreover be divulged because of the expiry of the two-year time-limit under section 34(1)(4) of that Act were likewise unavailing, because that Act did not apply retroactively.

G. The judgment of the Supreme Administrative Court in case no. 996/2004

50. In a final judgment of 15 May 2004 (реш. № 4408 от 15 май 2004 г. по адм. д. № 996/2004 г.), given pursuant to an appeal by the same person as in case no. 9881/2003 (see paragraph 49 above), concerning a further refusal to inform him of measures of covert surveillance against him, the Supreme Administrative Court held that his request for such information had properly been denied, because the information relating to special means of surveillance and the intelligence obtained by using them was a state secret within the meaning of section 25 of the PCIA and points 6 and 8 of part II of Schedule No. 1 to the PCIA (see paragraphs 43-45 above). On the other hand, the eventual intelligence obtained pursuant to a warrant to use special means of surveillance, as well as the warrant itself, were an official secret within the meaning of section 26(1) of the PCIA. This followed also from the prohibition to divulge information about special means of surveillance laid down in section 33 of the SSMA. The court went on to hold that the fact that the use of special means of surveillance could only be authorised by the presidents of the regional courts was sufficient to ensure independent judicial review of the activities of the executive and provided sufficient safeguards against unwarranted restriction on the citizens' rights.

H. The Criminal Code of 1968

51. Article 145a § 1 of the Criminal Code of 1968 criminalises the use of information obtained through special means of surveillance for ends other than protecting national security or combating crime. The offence is aggravated if it has been committed by officials who have acquired or have come across this information in connection with the performance of their duties (paragraph 2 of that Article). It is furthermore an offence to

unlawfully use information obtained through such means with a view to misleading a judicial authority (Article 287a § 1 (4) of the Code). There is no reported case-law on the application of these texts.

I. Relevant official reports and newspaper publications

- 52. In the end of 2000 the Supreme Cassation Prosecutor's Office carried out a special inquiry on the use of special means of surveillance by the Ministry of Internal Affairs during the period 1 January 1999 – 1 January 2001. While the inquiry was pending, the prosecutor in charge gave an interview, published in the daily *Trud* on 24 November 2000, in which he said that the Ministry of Internal Affairs was obstructing the inquiry. The report of the inquiry, which was finalised in January 2001, was presented to the National Assembly, the Council of Ministers, the Supreme Judicial Council and the Ministry of Internal Affairs, but was apparently not made available to the general public. Nevertheless, some of the report's findings were leaked to and reported by several daily newspapers. The report stated that the overall number of warrants for the use of special means of surveillance during the period 1 January 1999 – 1 January 2001 was just over 10,000, and that not including tapping of mobile phones. Out of these, only 267 or 269 had subsequently supplied evidence for use in criminal proceedings. In 243 cases special means of surveillance had been used against persons in respect of whom there had been no grounds for suspecting that they had committed a serious intentional offence. In a number of cases the orders for the deployment of such means had not been signed by the Minister of Internal Affairs himself, but by unknown persons on his behalf. In 36 cases the dates of the applications for warrants and of the warrants themselves had been modified. In 28 cases the warrants had not been assigned a number. In some cases the warrants had authorised measures implemented more than twenty-four hours before their issue. In two cases the persons in respect of whom the warrants had been issued were not the persons under investigation.
- 53. In an interview published by the daily *Trud* on 26 January 2001 the Minster of Internal Affairs said that during his thirteen months in office he had signed 4,000 orders for the use of special means of surveillance.
- 54. During the period December 2002 February 2003 various newspaper publications reported a number of cases where it was alleged that the services of the Ministry of Internal Affairs had unlawfully used special means of surveillance. The allegations included illegal tapping of the telephones of opposition leaders, journalists, a former constitutional court judge, and other judges. In an interview published on 11 December 2002 the Minister of Justice stated that "a tremendously high number of wiretappings take place in Bulgaria, but apparently for aims different from those of the criminal process".

THE LAW

I. ADMISSIBILITY

A. The parties' submissions

- 55. The Government disputed the applicant association's status as a victim within the meaning of Article 34 of the Convention. In their view, legal persons could not invoke the protection of Article 8 of the Convention. The Government relied on the former Commission's decision in the case of *Scientology Kirche Deutschland v. Germany* (no. 34614/97, Commission decision of 7 April 1997, unreported).
- 56. The applicants replied that even if it were to be admitted that legal persons could not have a private or family life within the meaning of Article 8 of the Convention, the same was not true of correspondence, in the form of mail or of telephone or electronic communications. They further pointed out that the applicant association was a "human rights watchdog". It mounted strategic human rights cases, which was often viewed with resentment and hostility by the authorities. Several lawyers, widely known for their criticism of the authorities, were working on staff. Domestic and international human rights organisations, as well as people seeking legal advice, some of whom were prisoners, accounted for a large part of its correspondence. There was therefore a reasonable likelihood that its communications - which in practice were indistinguishable from those of the lawyers working for it – could have been monitored. Moreover, as these communications were between lawyers and clients and their monitoring could have an incidence on the rights enshrined in Article 6 of the Convention, the Court had to apply a more rigorous standard in assessing the potential interference with them.

B. The Court's assessment

57. Article 34 of the Convention provides, as relevant:

"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. ..."

58. The Court considers that this case closely resembles the cases of Klass and Others v. Germany, Malone v. the United Kingdom, and Weber and Saravia v. Germany. In all these cases the Court found that to the extent that a law institutes a system of surveillance under which all persons in the

country concerned can potentially have their mail and telecommunications monitored, without their ever knowing this unless there has been either some indiscretion or subsequent notification, it directly affects all users or potential users of the postal and telecommunication services in that country. The Court therefore accepted that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them, without having to allege that such measures were in fact applied to him or her (see *Klass and Others*, judgment of 6 September 1978, Series A no. 28, pp. 16-20, §§ 30-38; *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, p. 31, § 64; and *Weber and Saravia v. Germany* ((dec.), no. 54934/00, §§ 78 and 79, ECHR 2006-...).

59. In line with its holdings in these cases, the Court finds that the second applicant, being an individual, can claim to be victim, within the meaning of Article 34, on account of the very existence of legislation in Bulgaria permitting secret surveillance. It notes in this connection that the applicants do not contend that measures of surveillance were actually applied to them; it is therefore inappropriate to apply a reasonable-likelihood test to determine whether they may claim to be victims of a violation of their Article 8 rights (see *Halford v. the United Kingdom*, judgment of 25 June 1997, *Reports of Judgments and Decisions* 1997-III, pp. 1018-19, §§ 55-57).

60. As regards the applicant association, the Court notes that it has already held that a legal person is entitled to respect for its "home" within the meaning of Article 8 § 1 of the Convention (see Société Colas Est and Others v. France, no. 37971/97, § 41, ECHR 2002-III; Buck v. Germany, no. 41604/98, § 31, 28 April 2005; and Kent Pharmaceuticals Limited and Others v. the United Kingdom (dec.), no. 9355/03, 11 October 2005). The applicant association is therefore, contrary to what the Government suggest, not wholly deprived of the protection of Article 8 by the mere fact that it is a legal person. While it may be open to doubt whether, being such a person, it can have a "private life" within the meaning of that provision, it can be said that its mail and other communications, which are in issue in the present case, are covered by the notion of "correspondence" which applies equally to communications originating from private and business premises (see Halford, cited above, p. 1016, § 44; Aalmoes and Others v. the Netherlands (dec.), no. 16269/02, 25 November 2004; and Weber and Saravia, cited above, § 77, with further references). The former Commission has already held, in circumstances identical to those of the present case, that applicants who are legal persons may fear that they are subjected to secret surveillance. It has accordingly accepted that they may claim to be victims (see Mersch and Others v. Luxembourg, nos. 10439-41/83, 10452/83 and 10512/83 and 10513/83, Commission decision of 10 May 1985, Decisions and Reports

- (DR) 43, p. 34, at pp. 113-14). The applicant association is therefore entitled to the protection afforded by Article 8.
- 61. Furthermore, unlike the situation obtaining in the cases of *Scientology Kirche Deutschland* (cited above) and *Herbecq and Association* "Ligue des droits de l'homme" v. Belgium (nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, DR 92-A, p. 92), the Article 8 rights in issue in the present case are those of the applicant association, not of its members. There is therefore a sufficiently direct link between the association as such and the alleged breaches of the Convention. It follows that it can claim to be a victim within the meaning of Article 34 of the Convention.
 - 62. The Government's objection must therefore be rejected.
- 63. The Court further considers that the application is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention, nor inadmissible on any other grounds. It must therefore be declared admissible.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

- 64. The applicants alleged that by giving the authorities a wide discretion to gather and use information obtained through secret surveillance and by failing to provide sufficient safeguards against abuse, the SSMA entailed by its very existence a violation of Article 8 of the Convention. Article 8 reads, as relevant:
 - "1. Everyone has the right to respect for his private ... life ... 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. The parties' submissions

65. The applicants conceded that the Constitution of 1991 and the SSMA provided a basis for the impugned interference with their Article 8 rights. However, they were of the view that this was not enough to justify the interference as being "in accordance with the law". The Court's case-law required a very detailed national law on secret surveillance, and was even more demanding when it came to monitoring of lawyers and their offices. Sections 16, 18(1) and 34 of the SSMA were particularly problematic in this respect. Indeed, in his dissenting opinion a constitutional court judge had found that section 34(1) of the SSMA, which entrusted control over the system of secret surveillance solely to the Minister of Internal Affairs, did

not provide sufficient safeguards against arbitrary interferences with the rights to private life and correspondence. This lack of effective control was further reinforced by the blurred provisions of section 34(2) of the SSMA. Similarly, section 30 of the Act gave the Minister full discretion to decide what to do with intelligence falling outside the scope of the initial application for the use of special means of surveillance. So did a number of other texts. Section 18 of the SSMA did not map out a procedure for informing the judiciary that surveillance had started without its prior sanction, nor a procedure for acquainting them with the intelligence gathered. Moreover, this provision allowed the Minister to make an unlimited number of consecutive orders for surveillance, thus making possible monitoring without judicial sanction for prolonged periods of time. The SSMA did not provide for judicial control of the destruction of material not used as evidence in criminal proceedings, nor for control over the obligation of the services deploying special means of surveillance to discontinue their use pursuant to the request of the agency which has requested them. The Act did not set out in detail the procedures for obtaining ex post facto judicial authorisation of surveillance ordered by the Minister of Internal Affairs in urgent cases, for transcribing the raw data obtained, and for destroying the unused data. It did not prohibit the issuing of consecutive warrants on the basis of the same facts, and thus allowed the circumvention of the six-month time-limit for surveillance.

- 66. Concerning the necessity of the interference, the applicants pointed out that the number of secret surveillance measures was extremely high, as evidenced by the report of the Supreme Cassation Prosecutor's Office and various interviews given by high-ranking officials. So was the number of breaches of the SSMA. Another material circumstance was the complete lack of notification of the persons concerned and the attendant impossibility of obtaining any information on the matter.
- 67. The Government submitted that the interference was allowed by the Constitution of 1991 and the SSMA and was intended to protect national security and prevent disorder and crime. By law, special means of surveillance could only be used in respect of a limited class of persons. There was a special procedure to safeguard against arbitrary action. It included a reasoned application to a judge, who was the only official with the power to authorise the use of special means of surveillance. Exceptions from this prior judicial control were only possible in urgent cases. Even in such cases the surveillance had to be ordered by the Minister of Internal Affairs and approved *ex post facto* by a judge. In 1997 the SSMA had been the subject of a challenge before the Constitutional Court, which had found it compatible with the Constitution of 1991. The fact that the law did not provide for the notification of the persons concerned was fully compatible with this Court's holding in the case of *Klass and Others* (cited above). The applicants' reliance on the report of the Supreme Cassation Prosecutor's

Office was misguided, because this report related only certain cases where the SSMA had been breached and was accordingly not pertinent for determining the issue before the Court in the instant case.

68. In sum, the Government were of the view that, while abuses could not fully be ruled out, the SSMA provided adequate guarantees against unlawful infringements of the rights of individuals. It was beyond doubt that averting and uncovering certain offences and protecting national security was unthinkable without the use of special means of surveillance. The SSMA kept the delicate balance between these aims and respect for the rights enshrined by Article 8 of the Convention.

B. The Court's assessment

1. Was there an interference

- 69. Having regard to its established case-law in the matter (see *Klass and Others*, p. 21, § 41; *Malone*, p. 31, § 64; and *Weber and Saravia*, §§ 77-79, all cited above), the Court accepts that the existence of legislation allowing secret surveillance amounts in itself to an interference with the applicants' rights under Article 8 of the Convention. Indeed, this point was not disputed by the parties.
- 70. It is therefore necessary to examine whether this interference is justified under the terms of paragraph 2 of that Article: whether it is "in accordance with the law" and "necessary in a democratic society" for one of the purposes enumerated in that paragraph.

2. Was the interference justified

- 71. The expression "in accordance with the law", as used in Article 8 § 2, does not only require that the impugned measure should have some basis in domestic law. It also refers to the quality of this law, demanding that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him or her, and compatible with the rule of law (see, among many other authorities, *Malone*, cited above, *Kruslin v. France*, judgment of 24 April 1990, Series A no. 176-A, p. 20, § 27; *Huvig v. France*, judgment of 24 April 1990, Series A no. 176-B, p. 52, § 26; *Kopp v. Switzerland*, judgment of 25 March 1998, *Reports* 1998-II, p. 540, § 55; and *Amann v. Switzerland* [GC], no. 27798/95, § 50, ECHR 2000-II).
- 72. It is obvious that the SSMA provides a legal basis for the interference. The first requirement does not therefore raise any problem.
- 73. The second requirement, that the law be accessible, does not raise any problem either.

74. As to the third requirement, the law's foreseeability and compatibility with the rule of law, the Court notes the following principles emerging from its case-law.

75. In the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence (see, among other authorities, *Malone*, cited above, p. 32, § 67; *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, *Reports* 1998-V, p. 1925, § 46 (iii); and *Khan v. the United Kingdom*, no. 35394/97, § 26, ECHR 2000-V). In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated (see *Kruslin*, p. 23, § 33; *Huvig*, p. 55, § 32; *Amann*, § 56 *in fine*; and *Weber and Saravia*, § 93, all cited above).

76. To ensure the effective implementation of the above principles, the Court has developed the following minimum safeguards that should be set out in statute law to avoid abuses: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their communications monitored; a limit on the duration of such monitoring; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which data obtained may or must be erased or the records destroyed (see *Weber and Saravia*, cited above, § 95, with further references).

77. In addition, in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection against arbitrary interference with Article 8 rights (see *Klass and Others*, cited above, pp. 25-26, §§ 54-56; *mutatis mutandis*, *Leander v. Sweden*, judgment of 26 March 1987, Series A no. 116, pp. 25-27, §§ 60-67; *Halford*, cited above, p. 1017, § 49; *Kopp*, cited above, p. 541, § 64; and *Weber and Saravia*, cited above, § 94). The Court must be satisfied that there exist adequate and effective guarantees against abuse. This 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 permit, carry out and supervise them, and the kind of remedy provided by the national law (see *Klass and Others*, cited above, p. 23, § 50).

78. Turning to the facts of the present case, the Court notes that, while in certain respects Bulgarian law fully comports with the above requirements, in other respects it falls short.

- 79. The SSMA circumscribes the purposes for which covert monitoring may be used: preventing or uncovering serious offences or protecting national security (see paragraph 10 above; see also *Klass and Others*, cited above, p. 24, § 51; and *Christie v. the United Kingdom*, no. 21482/93, Commission decision of 27 June 1994, DR 78-A, p. 119, at pp. 121-22). Moreover, such monitoring may be used only if there are grounds to suspect that a serious offence is being planned or is or has been committed, and only if the establishment of the facts by other methods are deemed unlikely to succeed (see paragraph 10 above; see also *Klass and Others*, cited above, p. 24, § 51). However, these latter requirements apparently apply only with regard to combating criminal conduct, not protecting national security (see paragraph 10 above).
- 80. Surveillance may only be allowed pursuant to a written application giving reasons, which may be made solely by the heads of certain services. The application must identify the persons or objects to be placed under surveillance. It must also set out the grounds for suspecting these persons of planning, or committing, or having committed an offence. Finally, the application must specify the duration of the proposed surveillance and the methods to be used, as well as all hitherto investigative steps (see paragraph 13 above).
- 81. The warrant authorising the surveillance can be issued only under the hand of the president or the vice-president of a regional court, a military regional court, or a court of appeals (see paragraphs 14 above). This judicial authorisation must in principle be given before the surveillance has taken place. It must also, as a rule, be followed by an order of the Minister of Internal Affairs or a specifically designated deputy (see paragraph 15 above).
- 82. Exceptions from the procedure outlined above are only possible in urgent cases: the authorisation is then given by the Minister of Internal Affairs or a specifically designated deputy. However, a judicial warrant must be issued not more than twenty-four hours after that (see paragraph 16 above). Despite the applicants' allegations, it is apparent that the SSMA envisages that this exception is to be used sparingly and only in duly justified cases.
- 83. Surveillance may be authorised for a maximum of two months. This time-limit may be extended, up to six months, only pursuant to a fresh application and warrant (see paragraph 19 above).
- 84. It thus seems that during the initial stage, when surveillance is being authorised, the SSMA, if strictly adhered to in particular, if care is taken not to stretch the concept of "national security" beyond its natural meaning (see *Christie*, cited above, p. 134; and, *mutatis mutandis*, *Al-Nashif v. Bulgaria*, no. 50963/99, § 124, 20 June 2002) –, provides substantial safeguards against arbitrary or indiscriminate surveillance. However, the Court must also examine whether such safeguards exist during the later

stages, when the surveillance is actually carried out or has already ended. On this point, it notes the following elements.

85. Unlike the system of secret surveillance under consideration in the case of Klass and Others (cited above, p. 31, § 70; see also Weber and Saravia, § 57), the SSMA does not provide for any review of the implementation of secret surveillance measures by a body or official that is either external to the services deploying the means of surveillance or at least required to have certain qualifications ensuring his independence and adherence to the rule of law. Under the SSMA, no one outside the services actually deploying special means of surveillance verifies such matters as whether these services in fact comply with the warrants authorising the use of such means, or whether they faithfully reproduce the original data in the written record. Similarly, there exists no independent review of whether the original data is in fact destroyed within the legal ten-day time-limit if the surveillance has proved fruitless (see, as examples to the contrary, Klass and Others, p. 11, § 20; and Weber and Saravia, § 100; and Aalmoes and Others, all cited above). On the contrary, it seems that all these activities are carried out solely by officers of the Ministry of Internal Affairs (see paragraphs 18, 21 and 22 above). It is true that the Code of 1974 provided, in its Article 111b § 6, that the judge who had issued a surveillance warrant had to be informed when the use of special means of surveillance has ended. So does Article 175 § 6 of the Code of 2005. It is also true that there is an obligation under section 19 of the SSMA to inform the issuing judge when the use of special means of surveillance has been discontinued before the end of the authorised period (see paragraphs 38 and 42 above). However, the texts make no provision for acquainting the judge with the results of the surveillance and do not command him or her to review whether the requirements of the law have been complied with. Moreover, it appears that the provisions of the Codes of 1974 and 2005 are applicable only in the context of pending criminal proceedings and do not cover all situations envisaged by the SSMA, such as the use of special means of surveillance to protect national security.

86. Another point which deserves to be mentioned in this connection is the apparent lack of regulations specifying with an appropriate degree of precision the manner of screening of the intelligence obtained through surveillance, or the procedures for preserving its integrity and confidentiality and the procedures for its destruction (see, as examples to the contrary, *Weber and Saravia*, §§ 45-50; and *Aalmoes and Others*, both cited above).

87. The Court further notes that the overall control over the system of secret surveillance is entrusted solely to the Minister of Internal Affairs (see paragraph 27 above) – who not only is a political appointee and a member of the executive, but is directly involved in the commissioning of special means of surveillance –, not to independent bodies, such as a special board

elected by the Parliament and an independent commission, as was the case in *Klass and Others* (cited above, p. 12, § 21 and pp. 24-25, § 53), or a special commissioner holding or qualified to hold high judicial office, as was the case in *Christie* (cited above, pp. 123-30, 135 and 137), or a control committee consisting of persons having qualifications equivalent to those of a Supreme Court judge, as was the case in *L. v. Norway* (no. 13564/88, Commission decision of 8 June 1990, DR 65, p. 210, at pp. 215-16 and 220). A dissenting judge in the Constitutional Court had serious misgivings about this complete lack of external control (see paragraph 36 above; and, *mutatis mutandis*, *Al-Nashif*, cited above, § 127).

88. Moreover, the manner in which the Minister effects this control is not set out in the law. Neither the SSMA, nor any other statute lays down a procedure governing the Minister's actions in this respect. The Minister has not issued any publicly available regulations or instructions on the subject (see paragraph 28 above). Moreover, neither the Minister, nor any other official is required to regularly report to an independent body or to the general public on the overall operation of the system or on the measures applied in individual cases (see, as examples to the contrary, *Klass and Others*, p. 12, § 21 *in limine* and p. 25, § 53; *Christie*, pp. 123-28 and 137; and *L. v Norway*, p. 216, all cited above).

89. The Court further notes that if the intelligence gathered falls outside the scope of the application for the use of special means of surveillance, it is the Minister of Internal Affairs who decides, discretionarily and without any independent control, what is to be done with it (see paragraph 24 above; see also, *mutatis mutandis*, *Kopp*, cited above, p. 543, § 74). By contrast, German law, as modified by the German Federal Constitutional Court, subjected the transmission of intelligence to other services to very strict conditions and entrusted the responsibility of checking the existence of these conditions to an official qualified to hold judicial office. Compliance with the relevant requirements was also reviewed by the special independent commission set up under German law (see *Weber and Saravia*, cited above, §§ 125-28).

90. Finally, the Court notes that under Bulgarian law the persons subjected to secret surveillance are not notified of this fact at any point in time and under any circumstances. According to the Court's case-law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy. However, as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned (see *Klass and Others*, p. 27, § 58; *mutatis mutandis*, *Leander*, p. 27, § 66; and, more recently, *Weber and Saravia*, § 135, all cited above). Indeed, the

German legislation in issue in the cases of *Klass and Others* and *Weber and Saravia*, as modified by the German Federal Constitutional Court, did provide for such notification (see *Klass and Others*, p. 8, § 11 and p. 11, § 19; and *Weber and Saravia*, §§ 51-54). The position in the *Leander* case was similar (see, *mutatis mutandis*, *Leander*, cited above, pp. 14-15, § 31).

- 91. By contrast, the SSMA does not provide for notification of persons subjected to surreptitious monitoring under any circumstances and at any point in time. On the contrary, section 33 of the SSMA, as construed by the Supreme Administrative Court, expressly prohibits the disclosure of information whether a person has been subjected to surveillance, or even whether warrants have been issued for this purpose (see paragraphs 26, 49 and 50 above). Indeed, such information is considered classified (see paragraphs 43-45, 49 and 50 above). The result of this is that unless they are subsequently prosecuted on the basis of the material gathered through covert surveillance, or unless there has been a leak of information, the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their Article 8 rights. Bulgarian law thus eschews an important safeguard against the improper use of special means of surveillance.
- 92. Having noted these shortcomings, the Court must now verify, in so far as the available information permits, whether they have an impact on the actual operation of the system of secret surveillance which exists in Bulgaria. In this connection, the Court notes that the Bulgarian Supreme Cassation Prosecutor's Office apparently found, in a report of January 2001, that numerous abuses had taken place. According to this report, more than 10,000 warrants were issued over a period of some twenty-four months, from 1 January 1999 to 1 January 2001, and that number does not even include the tapping of mobile telephones (for a population of less than 8,000,000). Out of these, only 267 or 269 had subsequently been used in criminal proceedings. A significant number of breaches of the law had been observed (see paragraph 52 above). Additionally, in an interview published on 26 January 2001 the then Minster of Internal Affairs conceded that he had signed 4,000 orders for the deployment of means of secret surveillance during his thirteen months in office (see paragraph 53 above). By contrast, in Malone (cited above, p. 25, § 53 and p. 36, § 79), the number of the warrants issued was considered relatively low (400 telephone tapping warrants and less than 100 postal warrants annually during the period 1969-79, for more than 26,428,000 telephone lines nationwide). These differences are telling, even if allowance is made for the development of the means of communication and the rise in terrorist activities in recent years. They also show that the system of secret surveillance in Bulgaria is, to say the least, overused, which may in part be due to the inadequate safeguards which the law provides. By contrast, in Klass and Others (cited above,

- p. 28, § 59) and in *Christie* (cited above, p. 137) there were no indications that the practice followed was not in strict accordance with the law.
- 93. Against this background, the Court concludes that Bulgarian law does not provide sufficient guarantees against the risk of abuse which is inherent in any system of secret surveillance. The interference with the Article 8 rights of the applicants was therefore not "in accordance with the law" within the meaning of paragraph 2 of that provision. This conclusion obviates the need for the Court to determine whether the interference was "necessary in a democratic society" for one of the aims enumerated therein (see *Malone*, p. 37, § 82; *Kruslin*, p. 25, § 37; *Huvig*, p. 57, § 36; and *Khan*, § 28, all cited above).
 - 94. There has therefore been a violation of Article 8 of the Convention.

III. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

95. The applicants alleged that owing to the lack of information on whether they had been subjected to secret surveillance they were prevented from seeking any redress therefor, in breach of Article 13 of the Convention. Article 13 reads:

"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."

- 96. Neither the applicants, nor the Government have made submissions on this complaint.
- 97. Article 13 of the Convention requires that where a person has an arguable claim to be the victim of a violation of the rights set forth in the Convention, they should have a remedy before a national authority in order both to have their claim decided and, if appropriate, to obtain redress (see, among many other authorities, *Leander*, cited above, p. 29, § 77 (a)).
- 98. Having regard to its findings under Article 8 of the Convention, the Court considers that the applicants' complaint has raised an arguable claim under the Convention and that, accordingly, they were entitled to an effective remedy in order to enforce their rights under that Article (ibid., p. 30, § 79).
- 99. According to the Convention organs' case-law, in the context of secret surveillance an effective remedy under Article 13 means a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in such a system (see *Klass and Others*, p. 31, § 69; *mutatis mutandis*, *Leander*, p. 30, § 78 *in fine*; and *Mersch and Others*, p. 118, all cited above). The Court must therefore verify whether there exist under Bulgarian law remedies which are effective in this limited sense. In this connection, the Court notes that review of surveillance may intervene at

three stages: when it is first ordered, while it is being carried out, or after it has been terminated.

100. It is obvious that when surveillance is ordered and while it is under way, no notification of the persons concerned is possible, as such notification would jeopardise the surveillance's effectiveness. They are therefore of necessity deprived of the possibility to challenge specific measures ordered or implemented against them. However, this does not mean that it is altogether impossible to provide a limited remedy - for instance, one where the proceedings are secret and where no reasons are given, and the persons concerned are not apprised whether they have in fact been monitored – even at this stage. Examples of such remedies may be found in Klass and Others, where individuals believing themselves to be under surveillance could, albeit in exceptional cases, complain to the commission overseeing the system of secret surveillance and also apply to the German Federal Constitutional Court (see Klass and Others, cited above, p. 31, § 70; see also Weber and Saravia, § 57), in Christie, where recourse was possible to a special tribunal (see Christie, cited above, pp. 122-23, 128-29 and 136-37), in Mersch and Others, where it was possible to appeal to the Council of State (see Mersch and Others, cited above, p. 118), and in L. v. Norway, where complaints were possible to a control committee (see L. v. Norway, cited above, pp. 216 and 220). By contrast, Bulgarian law does not provide any such mechanism, nor does it contain, as already found (see paragraphs 84-92 above), a sufficiently effective apparatus for controlling the use of special means of surveillance.

101. As regards the availability of remedies after the termination of the surveillance, the Court notes that, unlike the legislation in issue in Klass and Others, and Weber and Saravia, as modified by the German Federal Constitutional Court (see Klass and Others, p. 8, § 11; and Weber and Saravia, §§ 51-54 and 136, both cited above), the SSMA does not provide for notification of the persons concerned at any point in time and under any circumstances. On the contrary, in two judgments of 12 February and 15 May 2004 the Supreme Administrative Court held that the information whether a warrant for the use of means of secret surveillance had been issued was not to be disclosed. The second judgment stated that such information was classified (see paragraphs 49 and 50 above). It thus appears, that, unless criminal proceedings have subsequently been instituted or unless there has been a leak of information, a person is never and under no circumstances apprised of the fact that his or her communications have been monitored. The result of this lack of information is that those concerned are unable to seek any redress in respect of the use of secret surveillance measures against them.

102. Moreover, the Government have not provided any information on remedies – such as an application for a declaratory judgment or an action for damages – which could become available to the persons concerned if

they find out about any measures against them (see *Hewitt and Harman v. the United Kingdom*, no. 12175/86, Commission's report of 9 May 1989, DR 67, p. 103, § 55). In *Klass and Others* the existence of such remedies was not open to doubt (see *Klass and Others*, p. 31, § 71; see also *Weber and Saravia*, § 61, both cited above).

103. In view of the foregoing considerations, the Court concludes that Bulgarian law does not provide effective remedies against the use of special means of surveillance. There has therefore been a violation of Article 13 of the Convention.

IV. ALLEGED VIOLATION OF ARTICLE 6 § 1 OF THE CONVENTION

104. The applicants complained under Article 6 § 1 of the Convention that because by law they were not to be apprised at any point in time of the use of special means of surveillance against them, they could not seek redress against that in the courts. Article 6 § 1 provides, as relevant:

"In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law."

105. Neither the applicants, nor the Government have made submissions on this complaint.

106. The first issue to be decided is the applicability of Article 6 § 1. The Court notes that it did not express an opinion on the matter in its judgment in the case of *Klass and Others*, where a similar complaint was made (see *Klass and Others*, cited above, pp. 32-33, § 75). However, the former Commission did rule on it in its report in the same case. It found that Article 6 § 1 was not applicable either under its civil or under its criminal limb (see *Klass and Others*, Report of the Commission, Series B no. 26, pp. 35-37, §§ 57-61). The Court does not perceive anything in the circumstances of the present case that can alter that conclusion.

107. There has therefore been no violation of Article 6 § 1 of the Convention.

V. APPLICATION OF ARTICLE 41 OF THE CONVENTION

108. 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

- 109. The applicants stated that they asked the Government to ensure that the legislation on the use of special means of surveillance be brought in line with the standards stemming from the Court's case-law within six months. Failing that, they claimed 5,000 euros (EUR) in non-pecuniary damages.
 - 110. The Government have not made submissions on these claims.
- 111. 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 (see, among other authorities, Assanidze v. Georgia [GC], no. 71503/01, § 198, ECHR 2004-II; and Ilaşcu and Others v. Moldova and Russia [GC], no. 48787/99, § 487, ECHR 2004-VII). Furthermore, in ratifying the Convention, the Contracting States undertake to ensure that their domestic law is compatible with it (see Maestri v. Italy [GC], no. 39748/98, § 47, ECHR 2004-I). The Court sees no reason to presume at this juncture that the Government will not comply with their obligation under Article 46 § 1 of the Convention to abide in a timely fashion by the Court's judgment, once it has become final and binding. It therefore sees no reason to make any award to the applicants.

B. Costs and expenses

- 112. The applicants did not make a specific claim for the reimbursement of costs and expenses and, stating that the case had involved a considerable amount of work, left the matter to the discretion of the Court.
 - 113. The Government did not express an opinion on the matter.
- 114. The Court notes that all the submissions in the case were drafted by the manager of the applicant association and by the second applicant. The Court cannot make an award in respect of the hours the applicants themselves spent working on the case, as this time does not represent costs actually incurred by them (see *Steel and Morris v. the United Kingdom*, no. 68416/01, § 112, ECHR 2005-II, with further references). On the other hand, the Court considers it reasonable to assume that the applicants have incurred certain expenses for the conduct of the proceedings. Ruling on an equitable basis, it awards them jointly EUR 1,000, plus any tax that may be chargeable.

C. Default interest

115. The Court considers it appropriate that the default interest 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 UNANIMOUSLY

- 1. *Declares* the application admissible;
- 2. Holds that there has been a violation of Article 8 of the Convention;
- 3. *Holds* that there has been a violation of Article 13 of the Convention;
- 4. *Holds* that has been no violation of Article 6 § 1 of the Convention;

5. Holds

- (a) that the respondent State is to pay the applicants jointly, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 1,000 (one thousand euros) in respect of costs and expenses, plus any tax that may be chargeable;
- (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* the remainder of the applicants' claim for just satisfaction.

Done in English, and notified in writing on 28 June 2007, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Claudia WESTERDIEK Registrar Peer LORENZEN
President