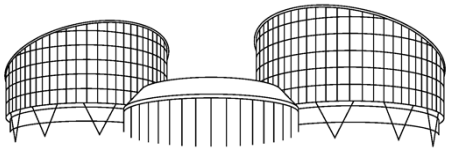

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

CASE OF EKIMDZHIEV AND OTHERS v. BULGARIA

(Application no. 70078/12)

JUDGMENT

Art 8 • Private life • Correspondence • Inadequate legal safeguards against arbitrariness and abuse for secret surveillance, retention and access of communications data

STRASBOURG

11 January 2022

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

TABLE OF CONTENTS

In the case of Ekimdzhiev and Others v. Bulgaria,

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

Tim Eicke, *President*,
Yonko Grozev,
Faris Vehabović,
Iulia Antoanella Motoc,
Armen Harutyunyan,
Gabriele Kucsko-Stadlmayer,
Ana Maria Guerra Martins, *judges*,
and Andrea Tamietti, *Section Registrar*,

Having regard to:

the application (no. 70078/12) 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") by two Bulgarian nationals, Mr Mihail Tiholov Ekimdzhiev and Mr Aleksandar Emilov Kashamov, and by two non-governmental organisations, the Association for European Integration and Human Rights and the Access to Information Foundation ("the applicants"), on 19 October 2012;

the decision to give the Bulgarian Government ("the Government") notice of the complaints under Articles 8 and 13 of the Convention concerning (a) the system of secret surveillance in Bulgaria and (b) the system of retention of communications data in Bulgaria and its subsequent access by the authorities, and to declare the remainder of the application inadmissible;

the parties' observations;

Having deliberated in private on 7 December 2021,

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

INTRODUCTION

1. The case concerns the compatibility of the Bulgarian laws and practices relating to (a) secret surveillance and (b) the retention of and access to communications data with Article 8 of the Convention.

THE FACTS

2. The four applicants are two lawyers and two non-governmental organisations related to them.

3. The first applicant, Mr Ekimdzhiev, was born in 1964 and lives in Plovdiv. He is a lawyer whose practice includes acting as counsel in various domestic cases and representing applicants before this Court.

4. The second applicant, the Association for European Integration and Human Rights, was founded in 1998 and has its registered office in Plovdiv. The first applicant, Mr Ekimdzhiev, is the chairman of its board.

5. The third applicant, Mr A.E. Kashamov, was born in 1971 and lives in Sofia. He is also a lawyer whose practice includes acting as counsel in various domestic cases and representing applicants before this Court.

6. The fourth applicant, the Access to Information Foundation, was set up in 1997 and has its registered office in Sofia. The third applicant, Mr A.E. Kashamov, is the head of its in-house legal team.

7. The first and second applicants were initially represented before the Court by Ms S. Stefanova and Ms G. Chernicherska, lawyers practising in Plovdiv, and then by, respectively, Ms T. Ekimdzhieva and Ms M. Dokova-Kostadinova, likewise lawyers practising in Plovdiv.

8. The third applicant was represented by Mr A.A. Kashamov, a lawyer practising in Sofia. The fourth applicant was represented by the third applicant, Mr A.E. Kashamov.

9. The Government were represented by their Agent, Ms M. Dimitrova of the Ministry of Justice.

10. The applicants asserted that the nature of their activities put them at risk of both secret surveillance and of having their communications data accessed by the authorities under the laws authorising that in Bulgaria. They did not allege that they had in fact been placed under surveillance or had had their communications data accessed by the authorities.

RELEVANT BULGARIAN LAW AND PRACTICE

I. SPECIAL MEANS OF SURVEILLANCE

A. Meaning of the term “special means of surveillance” and most common types of surveillance techniques

11. In Bulgaria, the umbrella term “special means of surveillance” comprises electronic or mechanical devices enabling the preparation of evidential materials (video and audio recordings, photographs and marked objects) and the covert techniques for using those devices (section 2(1) and (2) of the Special Surveillance Means Act 1997 and Article 172 § 1 of the Code of Criminal Procedure). Those techniques are (a) visual surveillance, (b) eavesdropping and tapping, (c) tracking, (d) covertly intruding (into vehicles or premises), (e) marking and checking correspondence or computerised information, (f) controlled delivery, (g) pseudo-transactions, and (h) the use of undercover agents (section 2(3) of the 1997 Act and Article 172 § 1 of the Code). Sections 5 to 10c define each of those techniques. Section 6 in particular clarifies that tapping and

eavesdropping include the interception of both telephone and electronic communications.

12. According to the annual reports published by the National Bureau for Control of Special Means of Surveillance (see paragraphs 14, 16 and 108 below) since 2014, the techniques which are used most often are (a) visual surveillance and (b) tapping and eavesdropping:

Year	Visual surveillance	Tapping or eavesdropping
2014	2,773 (24.94%)	4,927 (44.33%)
2015	1,417 (20.25%)	3,848 (54.97%)
2016	1,865 (21.56%)	4,717 (54.80%)
2017	1,699 (21.23%)	4,470 (55.86%)
2018	1,669 (19.39%)	5,124 (59.53%)
2019	1,628 (19.22%)	5,076 (59.92%)
2020	1,372 (18.27%)	4,594 (61.19%)

B. General outline and evolution of the relevant legislation

13. Special means of surveillance were first regulated in Bulgaria with the Special Means of Surveillance Act 1994, in force until 1997. Currently, the law governing special means of surveillance is chiefly set out in the Special Means of Surveillance Act 1997, as amended, Articles 172-177 of the Code of Criminal Procedure, as amended, sections 304-310 of the Electronic Communications Act 2007, as amended, and the internal rules of the National Bureau for Control of Special Means of Surveillance, whose most recent version was adopted in October 2016.

14. In December 2008, following the Court's judgment in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (no. 62540/00, 28 June 2007), in which the Court found breaches of Article 8 and 13 of the Convention, the 1997 Act was extensively amended. The explanatory notes to the amendment bill referred to that judgment and the need to bring the Act into line with the requirements of the Convention. Along with a host of other changes, the amendment created a National Bureau for Control of Special Means of Surveillance ("the National Bureau"), an independent authority whose five members were to be elected by Parliament and whose task was to oversee the use of special means of surveillance and the storing and destruction of material obtained through such means, and to protect individuals against the unlawful use of such means.

15. In October 2009, however, before the National Bureau could start operating, Parliament enacted further amendments to the 1997 Act, abolishing the Bureau and replacing it with a special parliamentary subcommittee. The amendments came into effect in November 2009. For

further details on these amendments and the committee's work in 2011, see *Hadzhiev v. Bulgaria* (no. 22373/04, §§ 26-28, 23 October 2012), and *Lenev v. Bulgaria* (no. 41452/07, §§ 81-83, 4 December 2012).

16. A further amendment to the 1997 Act which came into effect in August 2013 re-established the National Bureau as an "independent State authority" (see paragraphs 108 to 123 below). Its five members were elected by Parliament in December 2013, and it began its work in the beginning of 2014. The special parliamentary subcommittee became a full committee and continued to exist alongside the Bureau (see paragraph 125 below).

17. The relevant provisions of all enactments cited in paragraph 13 above, and of all other relevant provisions mentioned in the text, are set out below as they stood on 7 December 2021.

C. Situations which may trigger the use of special means of surveillance

18. Special means of surveillance may be used if that is necessary to prevent or detect one or more of the "serious intentional offences" (Article 93 § 7 of the Criminal Code defines a "serious" offence as one punishable by more than five years' imprisonment) listed in an exhaustive manner in section 3(1) of the 1997 Act and Article 172 § 2 of the Code of Criminal Procedure, which refer either to the chapters in the Criminal Code in which the provisions defining those offences are contained or to the provisions themselves.[1] Those include various offences against the Republic (such as attempted *coup d'état*, treason, espionage and sabotage); terrorist offences, including preparatory ones; murder; causing grievous bodily harm; abduction; rape and some other sexual offences; human trafficking; vote buying and some other electoral offences; theft; robbery; embezzlement; fraud; blackmail; dealing in stolen goods; money laundering; various economic, credit and customs offences; aggravated forgery; aggravated misuse of public office; perverting the course of justice; bribery; being the leader or member of a criminal gang; some aggravated computer offences; arson; some transport offences; some ecological offences; various narcotic drugs offences; disclosing official secrets; desertion in wartime and various military offences; unlawfully dealing in nuclear materials; and various offences against peace and humanity.

[1] A slight difference exists between the two lists: the offence under Article 320 § 2 of the Criminal Code (overt incitation towards an act of terrorism or a preparatory offence) features in section 3(1) of the 1997 Act but not in Article 172 § 2 of the Code of Criminal Procedure.

19. According to the National Bureau's annual reports, the two offences which have given rise to the highest number of instances of surveillance since 2014 were those under Article 321 of the Criminal Code (being the leader or a member of a criminal gang, which, regardless of its place of commission within Bulgaria, has been within the jurisdiction of the Specialised Criminal Court since that court's creation in 2011-12 – see paragraph 46 below) and under Article 354a of the Code (dealing in narcotic drugs, which, if committed by criminal gangs, has likewise been within the jurisdiction of the Specialised Criminal Court since its creation in 2011-12):

Year	Criminal gangs	Narcotic drugs
2014	20.90%	29.30%
2015	34.15%	19.00%
2016	42.05%	14.00%
2017	43.52%	14.63%
2018	53.17%	14.28%
2019	48.78%	14.91%
2020	51.11%	13.86%

20. The additional condition is that special means of surveillance may be used to prevent or detect one or more of those offences only if the requisite intelligence cannot be obtained by other means, or if doing so would entail exceptional difficulties (section 3(1) *in fine* of the 1997 Act).

21. When deployed to prevent or detect such offences, special means of surveillance are to be used to obtain evidence about them (section 3(2)).

22. Special means of surveillance may also be used for activities relating to national security (section 4 of the 1997 Act).[2] The Government submitted that in practice national security was never cited as a standalone ground for surveillance, and that surveillance applications were always also based on the need to prevent or detect an offence. They cited two statements drawn up by the National Bureau and the State Agency for National Security for the purposes of the present proceedings. In its statement, the Bureau said that in its inspections it had found that authorities seeking the use of special means of surveillance always referred to a relevant offence. In its statement, the State Agency for National Security said that owing to the manner in which section 14(1) and (3) of the 1997 Act (see paragraphs 39 and 41

[2] Section 2 of the Management and Functioning of the System for Protecting National Security Act 2015 defines "national security" as "a dynamic state of society and the State in which territorial integrity, sovereignty and constitutional order are protected, and the democratic functioning of the institutions and the fundamental rights and freedoms of citizens are guaranteed, as a result of which the nation preserves and increases its welfare and develops, and the country successfully protects its national interests and realises its national priorities".

below) was to be construed, surveillance applications always had to refer to a relevant offence.

D. Persons who or objects which can be subjected to secret surveillance

1. General rules

23. By section 12(1) to (3) of the 1997 Act, special means of surveillance may be used with respect to (a) persons suspected of, or unwittingly used for, the preparation or commission of one or more of the above-mentioned "serious intentional offences"; (b) persons or objects related to national security; (c) objects necessary to identify such persons; (d) persons who have agreed to being placed under surveillance to protect their life or property; or (e) a witness in criminal proceedings who has agreed to being placed under surveillance in order to expose the commission of one of the offences listed in section 12(3) by another (those include terrorist offences, hostage holding, human trafficking, taking and giving a bribe, and being the leader or member of a criminal gang).

24. According to the National Bureau's annual reports, the number of persons placed under surveillance each year since 2011 were as follows:

Year	Persons placed under surveillance	Of those, of their own volition
2011	8,184	not specified
2012	5,902	not specified
2013	4,452	not specified
2014	4,202	162
2015	2,638	79
2016	2,749	73
2017	2,748	55
2018	3,046	62
2019	3,310	not specified
2020	3,042	not specified

25. According to the National Bureau's annual reports, the number of cases in which the authorities had placed under surveillance objects with a view to identifying persons (see paragraph 23 (c) above) were as follows:

Year	Number of cases in which objects were placed under surveillance for identification purposes
2014	645
2015	299
2016	340
2017	261

Year	Number of cases in which objects were placed under surveillance for identification purposes
2018	279
2019	259
2020	172

2. Rules relating to lawyer-client communications

26. By section 33(1) of the Bar Act 2004, lawyers' papers, files, electronic documents, computer equipment and other data carriers are "inviolable" and are not subject to inspection, copying, checks or seizure. By section 33(2), correspondence between lawyers and clients, regardless of the means of communication, electronic or otherwise, is not subject to inspection, copying, checks or seizure either. By section 33(3), conversations between a lawyer and a client cannot be intercepted and recorded, and any possible recordings of such conversations cannot be used as evidence and are subject to immediate destruction. By Article 136 § 2 of the Code of Criminal Procedure, the use of special means of surveillance with respect to lawyers is subject to the requirements of the 2004 Act. The Supreme Court of Cassation has held that in spite of the literal terms of section 33(3) of the 2004 Act, the prohibition which it lays down is not necessarily absolute in all cases, in view of, among other things, the public interest in detecting offences committed by lawyers (see реш. № 211 от 08.04.2019 г. по н. д. № 1009/2018 г., ВКС, III н. о.). The 1997 Act does not contain any provisions specifically dealing with the surveillance of lawyers or the interception of their communications as a result of the surveillance of their clients.

27. The issue appears to have been touched upon solely in an instruction issued by the Chief Prosecutor on 11 April 2011 in the exercise of his power under section 138(4) (since August 2016, section 138(6)) of the Judiciary Act 2007 to make instructions governing the work of the prosecuting authorities. The instruction's preamble said that its issuing was necessary to halt inconsistent practices and avert breaches of section 33 of the 2004 Act (see paragraph 26 above).

28. Point 12 of the instruction says that special means of surveillance can be used with respect to lawyers only if there is information which can provide grounds for a reasonable suspicion that they have, alone or with others, committed an offence. The surveillance request must expressly mention that the surveillance will be directed against a lawyer.

29. Point 13 of the instruction says that if in the course of a surveillance operation the authorities record the conversation of a lawyer with a client or with another lawyer, and that conversation touches upon a client's defence, they must not prepare evidentiary material on its basis, unless the

surveillance reveals that the lawyer has him- or herself engaged in criminal activity.

30. It does not seem that the instruction has been published by the Prosecutor's Office. On 13 April 2011 the Chief Prosecutor did, however, send a copy of it to the Supreme Bar Council, and in June 2011 the Supreme Bar Council published it in issue 5-6/2011 of its journal, "Lawyers' Review" (*Адвокатски преглед*) (link).

E. Authorisation procedures

1. Authorities entitled to request secret surveillance

31. Only a limited number of authorities may seek the use of special means of surveillance and draw on the intelligence obtained thereby, within the spheres of their respective competencies.

32. Outside the framework of already pending criminal proceedings, the use of such means may only be sought by: (a) various directorates of the Ministry of Internal Affairs (national police, fight against organised crime, border police, internal affairs, regional directorates and various specialised directorates); (b) the territorial directorates and units of the State Agency for National Security; (c) the military-intelligence and military-police services attached to the Minister of Defence; (d) the Intelligence Agency; (e) regional prosecutor's offices (only in relation to serious electoral offences); and (f) the specialised anti-corruption directorate[3] (section 13(1) of the 1997 Act).

33. In the course of criminal proceedings, that may be done by the public prosecutor in charge of supervising the pre-trial investigation (section 13(2) of the 1997 Act and Article 173 § 1 of the Code of Criminal Procedure).

34. For the prevention of terrorist offences (including preparatory ones), the request may be made by the Chief Prosecutor, the head of State Agency for National Security, the head of the Intelligence Agency, the head of the military intelligence service (or their duly authorised deputies), or the chief secretary of the Ministry of Internal Affairs (section 13(4) of the 1997 Act).

35. Special rules govern offences alleged to have been committed by court presidents, judges, public prosecutors or investigators (section 13(3) of the 1997 Act and Article 174 § 5 of the Code of Criminal Procedure).

36. No other authorities may seek the use of special means of surveillance (section 13(6) of the 1997 Act).

37. The application must originate from the head of the respective authority; if it is made by a public prosecutor, he or she must notify the head

[3] That directorate forms part of the Commission for Combatting Corruption and Forfeiture of Unlawfully Acquired Assets (see *Todorov and Others v. Bulgaria*, nos. 50705/11 and 6 others, § 92, 13 July 2021).

of the respective prosecutor's office (sections 13(5) and 14(1) of the 1997 Act and Article 173 § 1 *in fine* of the Code of Criminal Procedure).

38. According to the National Bureau's annual reports, the respective share of surveillance applications were as follows:

Year	Ministry of Internal Affairs	State Agency for National Security	Prosecuting authorities	Other authorities
2014	43.40%	31.50%	24.90%	0.20%
2015	50.29%	19.16%	30.05%	0.51%
2016	56.22%	10.08%	33.39%	0.32%
2017	56.50%	6.41%	36.94%	0.15%
2018	60.78%	4.82%	34.27%	0.66%
2019	53.73%	5.69%	37.95%	2.63%
2020	51.12%	7.28%	36.98%	3.70%

2. Content of an application for secret surveillance

(a) The application itself

39. Surveillance applications made outside the framework of already pending criminal proceedings must be duly reasoned and set out (a) a full account of the circumstances giving cause to suspect that a relevant offence is being prepared or committed or has been committed, including when it comes to national security within the meaning of section 4 of the 1997 Act (see paragraph 22 above); (b) a full account of the steps already taken and the results of any previous preliminary inquiries or investigations; (c) data permitting the identification of the target (person or object); (d) the intended duration of the surveillance and reasons why that duration is necessary; (e) the intended surveillance techniques; (f) reasons why the intelligence cannot be obtained by other means or an account of the exceptional difficulties which that would entail; and (g) the official who will be informed of the results of the surveillance (section 14(1) of the 1997 Act).

40. Surveillance applications made in the course of criminal proceedings must also be duly reasoned and set out (a) information about the offence under investigation; (b) an account of all earlier investigatory steps and their results; (c) data permitting the identification of the target (person or object); (d) the intended surveillance techniques; (e) the intended duration of the surveillance and reasons why it is necessary; and (f) reasons why the intelligence cannot be obtained by other means or an account of the exceptional difficulties which that would entail (Article 173 § 2 of the Code of Criminal Procedure).

41. Surveillance applications relating to terrorist offences (including preparatory ones) must set out (a) the circumstances which give cause to suspect that a relevant offence is being prepared or committed or has been

committed; (b) if available, data permitting the identification of the target (person or object); (c) the intended duration of the surveillance; (d) the intended surveillance techniques; and (e) the official who will be informed of the results of the surveillance (section 14(3) of the 1997 Act).

42. Renewal applications must additionally contain a full account of any surveillance results obtained so far (section 21(3) of the 1997 Act and Article 173 § 6 of the Code of Criminal Procedure).

43. Applications concerning the surveillance or people for their own benefit, or of cooperating witnesses (see paragraph 23 (d) and (e) above), must be accompanied by their written consent (section 14(2) of the 1997 Act and Article 175 § 5 of the Code of Criminal Procedure).

(b) Materials supporting the application

44. For applications made outside criminal proceedings, the rule is that the requesting authority must enclose all materials on which its application is based (section 15(3) of the 1997 Act).[4] For applications made in the course of criminal proceedings, the rule is that the judge competent to issue the surveillance warrant may request those materials (Article 174 § 4 of the Code of Criminal Procedure).[5] It is unclear whether there is a difference in practice.

45. The National Bureau's annual report for 2017 – the only one to have touched upon the point – said (at p. 19) that in that year 2% of the applications made by the Ministry of Internal Affairs, 4% of those made by the prosecuting authorities, and 4% of those made by the State Agency for National Security had been refused because they had not presented all materials on which those applications had been based. According to the same report, the percentage of applications refused for that reason during the two preceding years had been 2.5% for the Ministry and 5% for the Agency in 2015, and 6% for the Agency in 2016.

3. Authorities competent to issue secret surveillance warrants

46. As a rule, surveillance warrants may be issued only by the presidents of the Sofia City Court, of the respective regional or military courts, and of the Specialised Criminal Court (which was created in 2011 and started its work in the beginning of 2012), or an expressly authorised deputy (section 15(1) and (2) of the 1997 Act and Article 174 §§ 1-3 of the Code of Criminal Procedure). The word "respective" – specifically added to

[4] Between 2013 and 2015, the rule was that the judge could request the production of those materials (section 15(2) of the 1997 Act, as worded between August 2013 and June 2015).

[5] The discrepancy appears to have arisen because the wording of Article 174 § 4 of the Code still matches that of section 15(2) of the 1997 Act before its amendment in June 2015 (they had been previously amended in parallel in August 2013), since the June 2015 amendment only concerned section 15 of the 1997 Act.

section 15(1) of the 1997 Act in 2013 to prevent the risk of forum-shopping by the relevant authorities – has been construed by the courts to mean the court which would be competent *ratione materiae*, *personae* and *loci* to try the alleged offence in relation to which surveillance is being sought (see реш. № 262304 от 07.04.2021 г. по гр. д. № 8701/2019 г., СГС, unclear whether final).

47. Special rules govern offences allegedly committed by judges, public prosecutors or investigators: in those cases the warrant may be issued by the presidents of the Sofia Court of Appeal, the Military Court of Appeal or the Specialised Criminal Court of Appeal, or a duly authorised deputy, depending on which court would be competent to try the criminal case (section 15(4)(1) of the 1997 Act and Article 174 § 5 of the Code of Criminal Procedure). If the offence is alleged to have been committed by one of those presidents or deputies, the warrant may be issued by the Vice-President of the Supreme Court of Cassation in charge of its Criminal Division (section 15(4)(2) of the 1997 Act and Article 174 § 6 of the Code of Criminal Procedure).

48. Compliance with those jurisdictional rules has been held to be an essential safeguard against unlawful surveillance (see реш. № 365 от 14.02.2014 г. по в. н. о. х. д. № 653/2013 г., САС, upheld by реш. № 189 от 03.02.2015 г. по н. д. № 515/2014 г., ВКС, II н. о.).

49. According to the National Bureau's annual reports (and, for the period 2011-14, the annual reports of the respective courts), the surveillance warrants issued by the presidents or vice-presidents of the four courts which had issued the largest number of those in 2015 were as follows:

Year	Sofia City Court	Specialised Criminal Court	Plovdiv Regional Court	Stara Zagora Regional Court
2011	6,008 (44.10%)	not applicable[6]	not specified	872 (6.40%)
2012	5,556[7]	550	not specified	498
2013	4,324	687	not specified	332
2014	2,298 (41.01%)	1,011 (18.04%)	not specified	not specified
2015	837 (21.38%)	1,049 (26.79%)	461 (11.78%)	240 (6.13%)
2016	90 (1.91%)	2,179 (46.25%)	485 (10.30%)	385 (8.17%)
2017	196 (4.24%)	1,808 (39.10%)	339 (7.33%)	320 (6.92%)
2018	190 (3.57%)	2,524 (47.71%)	333 (6.25%)	258 (4.84%)
2019	146 (2.71%)	3,006 (55.71%)	355 (6.58%)	271 (5.02%)
2020	120 (2.40%)	2,798 (55.93%)	422 (8.43%)	206 (4.12%)

[6] The Specialised Criminal Court started its work in 2012 (see paragraph 46 above).

[7] No data about the overall number of surveillance warrants issued in Bulgaria in 2012 and 2013 is publicly available.

50. In its annual report for 2016 (at p. 13), the National Bureau noted that although it was getting the largest number of surveillance applications in the country, the Specialised Criminal Court was not adequately staffed and resourced to deal with them properly. An inspection by the Bureau had revealed that that court was not in a position to process correctly the enormous volume of documents relating to such applications. The Bureau drew attention to the problem in its report for 2017 as well (at p. 16). In its report for 2019, the Bureau noted (at p. 16) that the large number of surveillance applications received by the Specialised Criminal Court on the one hand enabled the relevant judges to gain more experience, but on the other hand led to excessive workload, which was conducive to errors. That finding was repeated in the report for 2020 (at p. 27).

4. Manner of examination of secret surveillance applications

(a) Relevant statutory provisions and case-law

51. Surveillance applications made outside the framework of already pending criminal proceedings must be examined by the competent court president or vice-president on the papers within forty-eight hours,[8] and that president or vice-president can either issue a warrant or refuse the application, and must give reasons for his or her decision (section 15(1) *in fine* of the 1997 Act). For terrorist offences, the time-limit for decision is twenty-four hours (section 15(2) of the 1997 Act). When the application is made in the course of criminal proceedings, the law does not lay down a time-limit for ruling on it,[9] but likewise requires a reasoned decision (Article 174 § 4 of the Code of Criminal Procedure).

52. Decisions to allow or refuse a surveillance application cannot be challenged before the administrative courts by way of a claim for judicial review (see опр. № 11281 от 28.10.2015 г. по адм. д. № 10354/2015 г., ВАС, V о.).

(b) Information about the courts' practices relating to the examination of secret surveillance applications emerging from the National Bureau's annual reports

53. From the National Bureau's annual reports for 2015 (at pp. 16 and 25), 2016 (at pp. 15-16 and 26), 2017 (at pp. 17 and 27) and 2020 (at p. 29), it emerges that in practice surveillance applications are sometimes

[8] Between June 2015 and November 2017, that time-limit was seventy-two hours (section 15(1), as worded between June 2015 and November 2017). Between August 2013 and June 2015, section 15 did not lay down any time-limits. Before August 2013, section 15(2), as worded since its original enactment in 1997, required the judge to rule on the surveillance application "immediately after [its] receipt".

[9] Article 174 § 4 (before 2011, § 3) of the Code of Criminal Procedure, as worded between its original enactment in 2005 and August 2013, likewise required the judge to rule on the surveillance application "immediately after [its] receipt".

allowed in part and refused in part: only as regards certain surveillance techniques, or as regards certain offences, if the application concerns several, or for a shorter duration than requested.

54. From the National Bureau's annual reports for 2015 (at p. 16), 2016 (at p. 16), 2017 (at pp. 17-19), 2018 (at pp. 15-16), 2019 (at p. 17) and 2020 (at pp. 22-34 and 29) it further emerges that when they refused applications, the judges explained concretely their reasons for doing so: that the application did not originate from a competent authority; that it was not addressed to a competent court; that it did not relate to a relevant offence; that it did not contain enough information to ground a suspicion that the intended surveillance target has been implicated in an offence, or enough reasons why the warrant was to be issued; that it did not explain why a particular surveillance technique was necessary; that (for renewal applications) it did not set out the results already obtained; or that it sought authorisation for surveillance outside the statutory time-limits. According to the Bureau's annual report for 2020 (at p. 9), the largest number of refusals during that year had been based on the absence of enough information in the surveillance application that the intended targets were implicated in an offence.

55. According to the National Bureau's annual reports, the judicial decisions to allow or refuse an application for a surveillance warrant each year since 2014 were as follows:

Year	Applications allowed	Applications refused
2014	7,604 (98.07%)[10]	150 (1.93%)
2015	4,034 (85.52%)	683 (14.48%)
2016	4,885 (80.16%)	1,209 (19.84%)
2017	4,624 (77.86%)	1,315 (22.14%)
2018	5,328 (87.36%)	771 (12.64%)
2019	5,396 (89.35%)	643 (10.65%)
2020	5,003 (93.20%)	365 (6.80%)

(c) Other official accounts of the courts' practices

(i) In the Sofia City Court in 2013-17

(α) Criminal and disciplinary proceedings against the President of the Sofia City Court

56. In early 2015 the President of the Sofia City Court, who had taken up her duties in 2011, was charged with wilfully issuing surveillance

[10] In its first annual report, that for 2014, the National Bureau said (at pp. 11-15) that 184 of those applications ought to have been refused by the respective judges because they had been tainted by irregularities. In its subsequent reports, the Bureau did not engage in such analysis.

warrants in the absence of the legal prerequisites. She was suspended from her posts as court president and judge, and in March 2015 resigned from the post of president. In early 2016 she was convicted of deliberately authorising the surveillance of an automated centralised police information system operated by the Ministry of Internal Affairs by the Ministry's internal security department for a period exceeding the statutory maximum, contrary to Article 284c of the Criminal Code (see paragraph 145 below). She was, however, acquitted of the additional charge that the police information system in question was not a proper "object" of surveillance within the meaning of section 12(1) of the 1997 Act (see paragraph 23 (c) above). The first-instance judgment, which was classified (прис. № 1 от 15.01.2016 г. по н. о. х. д. № С-61/2015 г., СГС) concerned a warrant which she had issued in March 2014. It was fully upheld on appeal (see реш. № 42 от 10.01.2017 г. по в. н. о. х. д. № 50/2016 г., САС (apparently not published), and реш. № 57 от 19.04.2017 г. по н. д. № 161/2017 г., ВКС, I н. о.).

57. Parallel to that, in March 2015 the Minister of Justice asked the Supreme Judicial Council to open disciplinary proceedings against the (by then former) President of the Sofia City Court and dismiss her from her post as a judge as well, based on allegations that she had rendered the system of prior judicial authorisations of secret surveillance in the Sofia City Court ineffective. The Supreme Judicial Council at first refused to open such proceedings, but on an application by the Minister in August 2015 the Supreme Administrative Court quashed that refusal (see опр. № 9195 от 03.08.2015 г. по адм. д. № 5340/2015 г., ВАС, VI о.), and the Supreme Judicial Council did open such proceedings. They were later stayed to await the determination of the criminal charges against the (by then former) court president (see paragraph 56 above). In May 2017, after her conviction had become final, the Supreme Judicial Council dismissed her from her post as a judge as well.

58. According to a declaration drawn up by the 2013-18 chairperson of the National Bureau (see paragraphs 109 and 112 below) in February 2020 for the purposes of the present proceedings, and produced by the applicants, the deputies of that President of the Sofia City Court had made "four times as many" violations of the same nature but had not been brought to account for any of them.

(β) April 2017 report by the Vice-Presidents of the Sofia City Court

59. In an *ad hoc* report published in April 2017, two Vice-Presidents of the Sofia City Court recorded a number of shortcomings in the way in which that court had handled surveillance applications addressed to it until about mid-2015. Some of those shortcomings were: (a) between 2009 and mid-2014 the relevant registers had been kept in a way not permitting to see which judge had dealt with a given application; (b) the record-keeping

relating to such applications had been highly unsatisfactory; (c) many applications had been allowed even though they had not contained any factual data enabling an assessment of their well-foundedness; (d) there had been many cases of duplication of applications and warrants issued in relation to the same person on the same day; (e) surveillance had been allowed many times with respect to foreign embassies, in breach of international diplomatic law; (f) many applications not referring to any criminal offence, or referring to irrelevant offences, had been allowed; (g) many applications which should have been addressed to other courts had been allowed; (h) until April 2015 all decisions allowing surveillance applications had not contained any reasons; (i) between April and August 2015 those decisions had, with a few exceptions, given only blanket and generalised reasons; (j) in many cases, the surveillance warrants had not been drawn up by the judges but by the requesting authority, and the judges had simply signed them; (k) until April 2015, the post-surveillance reports required to be submitted by surveillance authorities (see paragraph 106 below) had not been brought to the attention of judges, and they had not taken any steps to review them; and (l) the competent judges had, in breach of their duties, failed to exercise any control over the destruction of irrelevant surveillance information.

60. The report went on to describe the steps taken after August 2015 to remedy those shortcomings and ensure the effective examination of all surveillance applications, such as: improved record-keeping; insisting in all cases that the requesting authority provide all materials supporting its application, and actual review of those materials by the judge; giving full reasons both when allowing and when refusing applications, including on whether the information in the supporting materials permitted a conclusion that the intended surveillance target was implicated in a relevant offence; and full control over the post-surveillance reports and the destruction of irrelevant surveillance materials.

(γ) Examples of surveillance warrants issued by the Sofia City Court in 2012-13

61. By way of example, the applicants submitted two surveillance warrants issued by the (then) President of the Sofia City Court in December 2012 and February 2013. Both were templates not mentioning any data about the specific case or about the people to be placed under surveillance, save for a reference to the number and date of the surveillance application, and both authorised the use of several surveillance techniques (visual surveillance, eavesdropping and tapping, and tracking), all for the maximum statutory time-limit of sixty days.[11]

[11] The term used by the law is “two months” (see paragraph 79 (c) and footnote 12 below).

(ii) In the Specialised Criminal Court in 2015-19

62. In his annual report for 2015, the President of the Specialised Criminal Court said (at pp. 1-2) that in the middle of the year the number of incoming surveillance applications had dramatically increased – according to him owing to the transfer of jurisdiction to try offences against the Republic (see paragraph 18 above) from the Sofia City Court to his court in June 2015. He and his deputy had thus been faced with a massive increase in their workload (see the table under paragraph 49 above). That is why he had asked the Supreme Judicial Council to appoint a second vice-president of the court.

63. In her annual report for 2018, the President *ad interim* of the Specialised Criminal Court said (at pp. 7-8) that her and her two deputies' had again faced a massive workload relating to surveillance applications, which had increased even more during that year (see the table under paragraph 49 above). The annual report for 2019 contained similar findings (at p. 5).

64. In a June 2019 judgment (прис. № 34 от 24.06.2019 г. по н. о. х. д. № 1907/2014 г., СпНС, unclear whether final), the Specialised Criminal Court described in some detail the content of eleven warrants issued either by the Vice-President of the Sofia City Court or the President or Vice-President of the Specialised Criminal Court in 2011-12. It noted that all of them were pre-printed forms with completely blanket contents and without any reference to the specific case to which they related except to the number of the surveillance application. The court further found that all those warrants had in fact been drawn up by others and simply signed by the respective judges, and concluded that there was no basis on which to accept that those judges had in fact verified the legal prerequisites for issuing the warrants.

65. In a December 2019 judgment (прис. № 55 от 09.12.2019 г. по н. о. х. д. № 1590/2019 г., СпНС), the Specialised Criminal Court made similar findings about nineteen surveillance warrants issued by the President and the two Vice-Presidents of that court in 2017-18. The court noted that all of the surveillance applications pursuant to which the warrants had been issued had contained detailed reasons why they were to be allowed. By contrast, the warrants themselves were all one-page documents which did not contain any reference (save for a reference to the numbers of the applications) to the individual cases to which they related, and which were couched in terms general enough to be capable of relating to any possible surveillance application under of the 1997 Act or under the Code of Criminal Procedure. Only the operative provisions of each of the warrants mentioned that the case concerned an alleged offence under Article 321 of the Criminal Code (see paragraph 19 above). All but one had allowed surveillance for the maximum statutory duration of two months, and all had authorised the use of several surveillance techniques: visual surveillance;

eavesdropping and tapping; tracking; and marking and checking correspondence or computerised information (see paragraph 11 above). It was thus impossible to speculate about whether the judges who had issued the warrants had in fact reviewed the applications for them (although the absence of review could not be presumed). The court also noted that its statistics for 2017-18 showed that it had on average received twelve or thirteen applications a day in 2017, and thirteen or fourteen applications a day in 2018, and that the practice of not giving individualised reasons was general. Based on its findings about the lack of proper reasons in the warrants, the court excluded the resulting evidence.

66. In February 2021 the Specialised Criminal Court of Appeal quashed that latter judgment. It held, among other things, that it could not be expected that in a decision to issue a surveillance warrant a judge would comment on the evidence. Neither the 1997 Act nor the Code of Criminal Procedure required that. All that the judge examining a surveillance application had to check was whether the formal requirements to allow it were in place (see реш. № 260002 от 10.02.2021 г. по в. н. о. х. д. № 245/2020 г., АСпНС, final).

67. Several leaks which emerged in the first half of 2021 suggested that between July 2020 and February 2021 many opposition politicians and journalists, as well as hundreds of participants in the 2020 anti-government protests in Bulgaria had been unjustifiably placed under secret surveillance on the basis of warrants issued by the Specialised Criminal Court in connection with allegations that they would attempt to carry out a *coup d'état*. When he spoke about the matter in Parliament on 28 July 2021, the Minister of Internal Affairs stated, among other things, that he had at his disposal documents showing that at least 123 protesters had been placed under surveillance on the basis of warrants issued by the Specialised Criminal Court, and expressed serious misgivings about the lawfulness of that surveillance, which in his view had been authorised uncritically by that court. In July 2021 Parliament set up an *ad hoc* committee to investigate the matter. The committee adopted its report on 13 September 2021; it has so far remained classified. On 15 September 2021 Parliament approved the report at a plenary sitting closed to the public.

(iii) Generally

68. In a February 2014 judgment, the Sofia Court of Appeal held that the use of boilerplate templates for decisions to issue surveillance warrants could be accepted, since, unlike the reasons to refuse a surveillance application, the reasons to allow one did not in practice vary (see реш. № 365 от 14.02.2014 г. по в. н. о. х. д. № 653/2013 г., САС, upheld by реш. № 189 от 03.02.2015 г. по н. д. № 515/2014 г., ВКС, II н. о.).

(d) Public reporting requirements

69. The presidents of regional and appellate courts and the President of the Supreme Court of Cassation must set out in the annual reports of their courts (a) the number of warrants issued and (b) the number of evidentiary materials drawn up based on that surveillance (section 29(8) of the 1997 Act).

5. Further vetting by the authorities deploying special means of surveillance

70. The only authorities having the power to deploy special means of surveillance are (a) the Technical Operations Agency attached to the Council of Ministers, (b) the Technical Operations Directorate of the State Agency for National Security, (c) the Intelligence Agency and the intelligence services of the Ministry of Defence (within their specific spheres of competence), and (d) (but only as regards undercover agents, controlled deliveries and pseudo-transactions) the Ministry of Internal Affairs (section 20(1) and (2) of the 1997 Act and Article 175 § 1 of the Code of Criminal Procedure). The explanatory notes to the 2013 bill (no. 354-01-19) which brought about the amendment to the 1997 Act which led to that position said that the reason to entrust most surveillance operations to a specialised structure separate from the Ministry of Internal Affairs was to ensure that those deploying special means of surveillance would be detached from those requesting them, and act independently and as a further safeguard against abuse.

71. When they receive a surveillance warrant, the head of the Technical Operations Agency, the head of the State Agency for National Security, the Secretary General of the Ministry of Internal Affairs, or a duly authorised deputy, as the case may be, must issue a follow-up order for the surveillance to go ahead (section 16(1) and (2) of the 1997 Act and Article 175 § 2 of the Code of Criminal Procedure). That additional step may be skipped in urgent cases, but the head of the respective authority, or the duly authorised deputy, must then be informed immediately (section 17 of the 1997 Act).

72. According to the National Bureau's annual reports, that additional step was skipped in the following number of cases:

Year	Follow-up order by head of respective authority skipped
2014	742 (17.70%)
2015	604 (22.09%)
2016	685 (25.28%)
2017	640 (23.29%)
2018	607 (19.93%)
2019	548 (16.56%)
2020	435 (14.38%)

73. Those surveillance authorities must not go ahead with the surveillance or must discontinue it if (a) the surveillance warrant has been issued with respect to an offence which is not among those listed in section 3(1) of the 1997 Act, or if (b) the surveillance application or the surveillance warrant contain obvious mistakes (section 22(3)(1) and (3)(2) of the 1997 Act). In such situations, the surveillance authority must notify the requesting authority and the judge who has issued the surveillance warrant. The judge must then cancel, vary or maintain the warrant, as the case may require, send his or her decision to the surveillance authority, and inform the requesting authority. If the judge varies or maintains the warrant, the surveillance operation must go ahead (section 22(5) of the 1997 Act).

74. In its annual report for 2015, the National Bureau said (at p. 17) that even before the amendments to the 1997 Act which introduced that additional safeguard had come into force in June and September 2015, it had instructed the surveillance authorities not to proceed with surveillance if they spotted such mistakes in surveillance applications or warrants.

75. According to the National Bureau's annual reports for 2016 (at p. 17), 2018 (at p. 17) and 2019 (at pp. 18-19), the surveillance authorities had triggered that additional safeguard in the following number of cases:

Year	**Referrals under section 22(3) of the 1997 Act**
2016	9
2018	3
2019	4

76. The Bureau's annual reports for 2014, 2015, 2017 and 2020 do not contain such information.

6. Retrospective authorisation in urgent cases

77. If there is an immediate risk that a serious intentional offence (among those listed in section 3(1) of the 1997 Act – see paragraph 18 above) is about to be committed, or a risk of an immediate threat to national security, special means of surveillance may be deployed without a judicial warrant, by order of the head of the Technical Operations Agency, the head of the State Agency for National Security, or the Secretary General of the Ministry of Internal Affairs (section 18(1) of the 1997 Act). The surveillance operation must stop if the competent judge has not issued a warrant within twenty-four hours; that judge must also decide whether any already obtained information is to be kept or destroyed (section 18(2)). If issued, the warrant retrospectively validates the surveillance steps taken before it has been issued (section 18(3)).

78. According to the National Bureau's annual reports, each year that urgent procedure was used with respect to the following number of persons:

Year	Persons placed under surveillance without a prior warrant
2014	125 (3.00%)
2015	29 (1.10%)
2016	49 (1.78%)
2017	28 (1.02%)
2018	7 (0.23%)
2019	15 (0.45%)
2020	4 (0.13%)

F. Maximum duration of secret surveillance

79. By section 21(1) and (2) of the 1997 Act and Article 175 §§ 3 and 4 of the Code of Criminal Procedure, the maximum amount of time during which special means of surveillance may be used is:

(a) up to twenty days, when used to identify persons (see paragraph 23 (c) above); this may be prolonged, by way of renewal applications, for up to a total of sixty days;

(b) up to two years, when used in relation to activities pertaining to national security (see paragraph 23 (b) above), to prevent serious intentional offences against the Republic; this may be prolonged, by way of renewal applications, for up to a total of three years;

(c) up to two months in all other cases (see paragraph 23 (a), (d) and (e) above); this may be prolonged, by way of renewal applications, for up to a total of six months.[12]

80. In its annual report for 2018, the National Bureau said that the two-year duration of the time-limit for surveillance on national-security grounds (see paragraph 79 (b) above) was one of the possible reasons for the reduced number of surveillance applications made by the State Agency for National Security since 2015 (see the table under paragraph 38 above).

81. The time-limit starts to run from the date set out in the surveillance warrant (section 21(4) of the 1997 Act).

G. Situations in which secret surveillance must be stopped

82. By section 22(1), (2) and (3) of the 1997 Act and Article 175 § 6 of the Code of Criminal Procedure, apart from the (special) cases when the surveillance authority must stop the surveillance if it finds that it concerns

[12] Until 2015, the duration was in all cases up to two months, with a possible prolongation of up to six months (section 21(1) and (2) of the 1997 Act, as worded between 1997 and 2015).

an irrelevant offence or that the surveillance application or warrant are tainted by an obvious mistake (see paragraph 73 above), the surveillance authority must stop the surveillance if (a) its permitted duration has expired; (b) its aims have been attained; (c) it does not yield results; (d) there is a risk that the techniques used for it will be revealed; or (e) it has become impossible.

83. In each of those cases, the surveillance authority must notify the judge who has issued the warrant (section 22(4) of the 1997 Act and Article 175 § 7 of the Code of Criminal Procedure). Section 22(4) requires notification to the requesting authority as well. Article 175 § 7 requires the notification to set out reasons in all possible cases, whereas section 22(4) only requires reasons if the surveillance has been stopped because (a) there was a risk that the techniques used for it would be revealed or (b) it has become impossible.

H. Processing of information obtained through special means of surveillance

1. Purposes for which the information may be used

84. The general rule is that information obtained through special means of surveillance may only be used to prevent, detect or prove criminal offences, or to protect national security (section 32 of the 1997 Act).

85. Using such information for another purpose is a criminal offence, which is aggravated if committed by a public official who has obtained access to the information by virtue of his or her office (Article 145a §§ 1 and 2 of the Criminal Code). It appears that so far there has been only one conviction under that provision, that of a high-ranking police officer who was leaking surveillance data to journalists and others (see прис. № 58 от 11.06.2014 г. по н. о. х. д. № 457/2012 г., ОС-Велико Търново, upheld in relevant part by реш. № 149 от 31.07.2015 г. по в. н. о. х. д. № 389/2014 г., АС-Варна, appeal on points of law withdrawn: see опр. Р-12 от 19.01.2016 г. по н. д. № 1372/2015 г., ВКС, III н. о.).

2. Means of acquiring electronic communications

86. For electronic communications, all communications service providers in the country are under a duty to enable the two main surveillance authorities (the Technical Operations Agency and Technical Operations Directorate of the State Agency for National Security – see paragraph 70 above) to have real-time access to all communications passing through their networks, so that those could be intercepted in line with the 1997 Act (section 304 of the Electronic Communications Act 2007). Communications service providers have the same duty to the courts and the investigating authorities (Article 172 § 3 of the Code of Criminal Procedure). They must at their own expense install and operate interfaces

which can automatically intercept and securely transmit communications to the surveillance authorities (sections 305(1), 308 and 309 of the 2007 Act).

3. Stages of processing

(a) "Primary recording" and "derivative data carrier"

87. Each covert surveillance technique (except the use of undercover agents – see реш. № 112 от 02.06.2016 г. по в. н. о. х. д. № 81/2016 г., ВтАС, upheld by реш. № 198 от 05.12.2016 г. по н. д. № 766/2016 г., ВКС, I н. о.) must result in a recording of the information obtained by it: a photograph, a video-recording, or an audio-recording (sections 11 and 24 of the 1997 Act).

88. The surveillance authority must keep the "primary recording" for as long as the surveillance operation is under way (section 25(6) of the 1997 Act). That "primary recording" is used to create a "derivative data carrier", which the surveillance authority must send to the requesting authority, along with (if requested by the latter) any photographs, records, blueprints or plans (section 25(1), (4) and (5)).

89. The "derivative data carrier" may be in writing or in another (in practice electronic) form (section 25(1) of the 1997 Act). If technically feasible, it must be made available to the requesting authority via an automated network (section 25(2)). Its content must fully match that of the "primary recording" (section 25(3)).

(b) Evidentiary material

90. If, based on that "derivative data carrier", the requesting authority finds that the surveillance has yielded useful information, it must immediately (and in any event not more than ten days after the surveillance has ended) advise the surveillance authority to prepare evidentiary material (*веществени доказателствени средства*) on the basis of the "primary recording" (sections 26 and 27(2) of the 1997 Act). Although the 1997 Act does not specify what exactly that evidentiary material consists of, from the criminal courts' case-law it transpires that it is computer files containing audio- or video-recordings, as the case may be (see, for instance, прис. № 50 от 03.06.2011 г. по н. о. х. д. № 424/2011 г., ОС-Варна, upheld in relevant part by реш. № 157 от 21.11.2011 г. по в. н. о. х. д. № 313/2011 г., ВнАС, and then by реш. № 83 от 19.06.2012 г. по н. д. № 3135/2011 г., ВКС, II н. о.; реш. № 172 от 18.04.2012 г. по н. д. № 398/2012 г., ВКС, I н. о.; прис. № 56 от 16.11.2016 г. по н. о. х. д. № 379/2014 г., ОС-Плевен, upheld by реш. № 124 от 03.05.2017 г. по в. н. о. х. д. № 69/2017 г., ВтАС, apparently not appealed against; and реш. № 1 от 17.02.2017 г. по н. д. № 1143/2016 г., ВКС, III н. о.). That evidentiary material is not to be confused with physical evidence (*веществени доказателства*), and the

court trying a criminal case cannot therefore lawfully order its destruction (see опр. № 145 от 17.06.2016 г. по в. ч. н. д. № 156/2016 г., ОС-Видин). When the surveillance authority prepares that evidentiary material, it must draw up a record setting out the time, place and physical conditions of the surveillance, the equipment and techniques used, any data obtained about the target, and the text of the evidentiary material (sections 27(1) and 29(4) of the 1997 Act and Article 132 § 2 of the Code of Criminal Procedure). In that record, it must also refer to the surveillance application, the surveillance warrant, and the follow-up order (and to the consent of the target, if the surveillance was carried out to protect a person or with respect to a cooperating witness) (section 29(3) of the 1997 Act and Article 132 § 3 of the Code of Criminal Procedure). Although the 1997 Act does not say that in terms, in practice that evidentiary material may not reproduce all parts of the "primary recording" (see, for instance, реш. № 384 от 08.07.2017 г. по в. н. о. х. д. № 1182/2016 г., САС, upheld by реш. № 314 от 25.01.2018 г. по н. д. № 1118/2017 г., ВКС, I н. о.). This also appears to follow from the rule that any parts of the "primary recording" which are not used for its preparation must be destroyed (see paragraph 94 below).

91. The evidentiary material must be prepared in two copies, one of which must be sent under seal to the requesting authority, and the other, again under seal, to the judge who issued the surveillance warrant. That must happen not more than twenty-four hours after they are prepared (section 29(1) of the 1997 Act and Article 176 § 1 of the Code of Criminal Procedure). The requesting authority may require additional copies of that material (section 29(1) *in fine* and Article 176 § 2).

92. Evidentiary material received by the requesting authority must be kept by it until criminal proceedings are opened in connection with it; when such proceedings are opened, the material is to be kept by the prosecutor's office and the court dealing with the case (section 31(1) and (2) of the 1997 Act). The Act does not lay down any rules on how that material is to be stored. According to the Government, the matter was regulated by internal rules of the relevant authorities, except for cases in which the material was for some reason regarded as classified, in which case its storage was governed by the relevant provisions of the Protection of Classified Information Act 2002 (see paragraphs 102 and 103 below). According to the Government, once criminal proceedings were opened, the evidentiary material was stored in accordance with the rules on the storage of evidence by the prosecuting authorities and the courts. Article 125 § 3 of the Code of Criminal Procedure provides that evidentiary material prepared on the basis of surveillance is to be placed in the case file of the criminal case. Neither the Rules on the administrative services of the courts, issued by the Supreme Judicial Council in 2017, nor the Rules on the administrative services of the prosecutor's offices, issued by the Supreme Judicial Council in 2013, which govern the storage of case files by,

respectively, the courts and the prosecuting authorities, contain provisions specifically dealing with the storage or destruction of evidentiary material prepared on the basis of surveillance.

93. According to the National Bureau's annual reports, the number of evidentiary materials produced on the basis of information obtained through surveillance and the ratio between those evidentiary materials and the number of persons placed under surveillance each year was as follows:

Year	Number of evidentiary materials	Ratio relative to the number of persons placed under surveillance
2010	3,461	60.06%
2011	3,603	44.02%
2012	3,347	56.71%
2013	1,602	48.38%
2014	1,084	24.46%
2015	1,677	57.10%
2016	1,431	46.33%
2017	1,670	55.52%
2018	1,714	56.27%
2019	1,124	33.96%
2020	1,089	36.01%

(c) Destruction of irrelevant information

94. If evidentiary material is prepared, (a) any parts of the "primary recording" which are not used for its preparation and (b) the "derivative data carrier" must be destroyed, both by the surveillance and by the requesting authority, within ten days after the end of the surveillance. That must be done and recorded by three-member commissions appointed by the heads of the respective authorities (section 31(3) of the 1997 Act).

95. If, conversely, the surveillance has not yielded any useful information, the surveillance authority does not have to prepare evidentiary material and must destroy any information obtained within ten days, in the same way as that set out in paragraph 94 above (section 28 read in conjunction with section 31(3) of the 1997 Act).

96. There are three reported cases in which police officers were given disciplinary punishments for failing to ensure the timely destruction of surveillance information (see реш. № 2466 от 11.10.2013 г. по адм. д. № 1804/2013 г., АдмС-Варна; реш. № 100 от 20.03.2019 г. по адм. д. № 708/2018 г., АдмС-Добрич; and реш. № 101 от 20.03.2019 г. по адм. д. № 709/2018 г., АдмС-Добрич).

97. In all cases in which the destruction of surveillance information is legally required, the surveillance authority must within seven days send the

record attesting the destruction to the requesting authority, along with the surveillance application and the surveillance warrant (section 31(4) of the 1997 Act). The requesting authority must then keep those (section 31(5)).

98. By way of exception to the normal destruction rules, any information obtained through surveillance on national-security grounds must be kept by the relevant requesting authority (the respective directorate of the State Agency for National Security, the military intelligence service attached to the Minister of Defence, and the National Intelligence Service) for fifteen years after the end of the surveillance (section 31(6) of the 1997 Act). It must after that be destroyed by a special three-member commission appointed by the head of the respective authority (section 31(7)).

99. All of the above rules on the destruction of information apparently apply only when the surveillance has taken place outside the framework of already pending criminal proceedings. When it has taken place in the course of criminal proceedings, the rule is that when the surveillance ends, the judge who has issued the warrant must be informed of its results. If any information obtained as a result of the surveillance is not used to prepare evidentiary material, that judge must order its destruction (Article 175 § 7 of the Code of Criminal Procedure). In its reports for 2015 (at p. 23), 2016 (at p. 21), 2019 (at p. 20) and 2020 (at p. 36), the National Bureau noted that the discrepancy between the two regimes sometimes caused delays in the destruction.

4. Rules on the permissible uses of surplus surveillance information

100. If the surveillance yields results which surpass the purpose for which it was originally sought, the head of the Technical Operations Agency or of the State Agency for National Security (depending on which one of the two has carried out the surveillance) must inform the relevant requesting authority of those surplus results within twenty-four hours (section 30(1) of the 1997 Act). The requesting authority must in turn inform the relevant authority within a further twenty-four hours (section 30(2)). A special rule governs the situation when the surplus results relate to the officer who has requested the surveillance or a superior of that officer: in that case, the head (or an expressly authorised deputy) of the relevant surveillance authority (the Technical Operations Agency, the State Agency for National Security, or the Ministry of Internal Affairs) must immediately send the surplus surveillance materials to the Chief Prosecutor or an expressly authorised deputy (section 30(3)).

101. Such surplus results may be used as evidence in criminal proceedings only if they concern another relevant serious intentional offence (Article 177 §§ 2 and 3 of the Code of Criminal Procedure).

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

102. Information about special means of surveillance (technical devices and/or the manner in which they have been used) used in the manner provided for by law is a State secret (point 6 of part II of Schedule No. 1 to the Protection of Classified Information Act 2002). Until 2013, so was information obtained as a result of the use of such means (point 8 of part II of Schedule No. 1). In 2013, point 8 was repealed.

103. In a 2014 interpretative decision dealing chiefly with the question whether the public could be excluded from hearings in criminal cases in which evidence obtained through special means of surveillance was being presented (тълк. реш. № 4 от 03.12.2014 г. по т. д. № 4/2014 г., ВКС, ОСНК), the Supreme Court of Cassation noted, among other things, that the effect of the repeal of point 8 was that the fact that evidentiary material had been prepared on the basis of information obtained through special means of surveillance was no longer in itself sufficient to treat that evidentiary material as classified information, even if it mentioned the type of means (visual surveillance, tapping, tracking, and so on) used to obtain the information.

104. In a statement enclosed with the Government's observations, the Technical Operations Agency (see paragraph 70 (a) above) said that according to its interpretation, the effect of point 6 of part II of Schedule No. 1 to the Protection of Classified Information Act 2002 was that both the "primary recording" obtained as a result of surveillance and the "derivative data carrier" were classified information (see paragraphs 87 and 88 above).

I. Authorities supervising the use of special means of surveillance

1. Judges who have issued the surveillance warrants

105. As noted in paragraph 83 above, when a surveillance operation ends, for whatever reason, the surveillance authority must notify judge who has issued the surveillance warrant.

106. Within one month after the end of a surveillance operation, the requesting authority must report to that judge. The report must specify the type of special means of surveillance used, the beginning and end of the surveillance, and whether the surveillance operation has resulted in the preparation of evidentiary material or whether the information obtained has been destroyed (section 29(7) of the 1997 Act). If evidentiary material has been prepared on the basis of the information obtained as a result of the surveillance (see paragraph 90 above), a copy of that evidentiary material, and of the accompanying records, must be sent, under seal, to that judge (see paragraph 91 above).

107. As noted in paragraph 99 above, for surveillance in the course of criminal proceedings, the judge who has issued the warrant must be

informed immediately after the end of the surveillance, and if the information obtained thereby is not used to prepare evidentiary material, he or she must order its destruction. The same judge must also receive a sealed copy of any evidentiary material resulting from a surveillance operation within twenty-four hours of its preparation (see paragraph 91 above).

2. National Bureau

108. The National Bureau – which was re-established as an "independent State authority" in 2013, was first elected in December 2013, and started its work in the beginning of 2014 (see paragraph 16 above) – is tasked with (a) supervising the procedures for authorising, deploying and using special means of surveillance, and the storage and destruction of the information obtained by such means, and with (b) protecting the rights of the persons affected by the unlawful use of such means (section 34b(1) of the 1997 Act). It is a permanent body assisted by its own administration (section 34b(4)). According to the Bureau's annual reports, in 2014-15 its administration had consisted of fifteen employees; in 2016-20, that number was reduced to fourteen; they all have the requisite security clearance ("top secret"). The Bureau must report annually to Parliament (section 34b(7)).

(a) Manner of election and term of office of the National Bureau's members

(i) Statutory provisions

109. The National Bureau has a chairperson, a deputy chairperson and three members, all elected by Parliament for five-year terms (section 34c(1) of the 1997 Act). They must have at least eight years of legal experience or experience in the law-enforcement or the security services, and must obtain the highest possible security clearance – "top secret" (section 34c(2) of the 1997 Act). Security clearances for that highest level of classification are issued after a special vetting procedure which must be carried out by the State Agency for National Security (section 49(1) and (2) of the Protection of Classified Information Act 2002).[13]

110. After the nominations for members of the National Bureau are received by Parliament (the 1997 Act does not say who can make those

[13] The general rule under section 36 of the Protection of Classified Information Act 2002 is that no official can access classified information unless holding the appropriate level of security clearance. The holders of a number of other posts (President of the Republic, Prime Minister, Chairperson of Parliament, government ministers, Secretary General of the Council of Ministers, members of Parliament, constitutional judges, judges, prosecutors, investigators, members of the Supreme Judicial Council and members of its Inspectorate, and lawyers in private practice) are, however, not subjected to such vetting and obtain a security clearance allowing them access to all levels of classified information (subject, however, to the "need to know" principle for all of them except the President of the Republic, the Prime Minister and the Chairperson of Parliament) automatically when they take up their duties (section 39(1) to (3) of the same Act).

nominations, but both in 2013 and in 2018 each of the nominations was made by a different parliamentary group, based on special rules of procedure adopted by Parliament on each of those occasions), the head of the specialised parliamentary committee sends all materials about the nominee to the State Agency for National Security for a security vetting, which must be completed within a month. After that the parliamentary committee examines the nominations within seven days, and then interviews the nominees considered eligible, and within a further seven days submits a report. After that Parliament votes on each of the nominees individually, and then chooses which ones among them will become chairperson and deputy chairperson. They are then all sworn in (section 34d of the 1997 Act).

111. After the end of their term of office, the members of the National Bureau they must be restored to their previous posts (section 34c(4)). Their terms of office may be terminated prematurely by Parliament if (a) they resign, (b) they have been in fact unable to carry out their duties for three months in a row, (c) they have ceased being eligible to occupy their post, or (d) they have been declared in conflict of interests following an official procedure under the special anti-corruption legislation (section 34c(6)).

(ii) Members of the National Bureau in 2013-18 and since 2018

112. Three out of the five original members of the National Bureau, elected in 2013, including its chairperson and its deputy chairperson, had legal education and legal experience. Only one of the members elected in December 2018 (who was a member during the 2013-18 term as well) had legal education and experience (as a lawyer in private practice). According to the Bureau's official website,[14] immediately before his election to the post in December 2018 the current chairperson had worked for ten years (2008-18) at the State Agency for National Security; the deputy chairperson elected in 2018 had also been employed for twenty-six years (1981-2007) by the security services; and one of the regular members had worked for many years (1983-2009) at the Ministry of Internal Affairs.

113. For the three regular members of the National Bureau, the current term of office (2018-23) is their second; all three were members in 2013-18 as well.

114. The National Bureau's original deputy chairperson, elected in 2013, had his term of office prematurely terminated by Parliament in March 2018 on the ground that he had ceased being eligible to be a member of the Bureau (see paragraph 111 (c) above) because in July 2017 the State Agency for National Security had revoked his security clearance (it later transpired that the reason cited for the revocation had been that he had disclosed information about the use of special means of surveillance to

[14] whttp://www.nbksrs.bg/за-нас/състав-на-бюрото/ (accessed on 30 July 2021)

several people, in breach of the legal requirement to keep such information secret), and in January 2018 the Supreme Administrative Court had finally upheld that revocation.[15]

115. In early June 2021 the National Bureau's deputy chairperson elected in 2018 was placed under various sanctions by the authorities of the United States of America pursuant to section 1(a)(ii)(B)(1) of Executive Order 13818 (Blocking the Property of Persons Involved in Serious Human Rights Abuse or Corruption), issued in 2017, and to section 7031(c) (Anti-Kleptocracy and Human Rights) of the annual Department of State, Foreign Operations, and Related Programs Appropriations Act owing, respectively, to his being "responsible for or complicit in, or ha[ving] directly or indirectly engaged in ... corruption", and to his being "involved in significant corruption". In mid-June 2021 he resigned from his post, and on 28 July 2021 Parliament unanimously accepted his resignation.

(b) Powers of the National Bureau

(i) To access materials

116. When carrying out its duties, the National Bureau may (a) seek relevant information from the authorities entitled to request surveillance, the judges dealing with surveillance applications, and the surveillance authorities, and (b) inspect the materials (surveillance applications, warrants and follow-up orders and records relating to the destruction of surveillance information) and registers kept by those authorities (section 34f(1)(1) and (1)(2) of the 1997 Act).

117. Both the members of the National Bureau and its employees can access (a) any documents relating to the use or deployment of special means of surveillance, (b) any documents relating to the storage or the destruction of materials obtained through such means, and (c) any premises containing such documents (section 34f(4) of the 1997 Act).

118. In its report for 2017, the National Bureau said (at p. 23) that the State Agency for National Security was not allowing it to inspect the materials which had prompted the surveillance applications made by it. The Agency was thus preventing effective supervision by the Bureau, since one of the aspects of that supervision was whether surveillance applications were based on genuine suspicions of criminal conduct. The Bureau also said (at p. 24) that owing to the many instances of provision of incorrect information by the Technical Operations Agency, in 2014-17 it had had to make repeat requests for information to that Agency in about 200 individual

[15] He has an application pending before the Court in relation to those matters (no. 34584/18), in which he complains under Articles 8 and 10 of the Convention of his dismissal from his post, and under Article 6 § 1 of the Convention of the alleged unfairness of the proceedings in which he challenged the revocation of his security clearance.

cases. It was hard for the Bureau to ascertain whether that had been a deliberate obstruction intended to conceal irregularities.

119. In November 2015 the Chief Prosecutor issued an instruction to all prosecutors about the manner in which the National Bureau was to be provided access to materials held by the prosecuting authorities in the course of its inspections. According to point 7 of that instruction (as partly amended in April 2019), members of the Bureau and its employees were to be given access to: surveillance applications, information notes enclosed with those, surveillance warrants (or judicial decisions to refuse to issue such warrants), follow-up surveillance orders, requests to stop surveillance, post-surveillance reports, documents attesting that surveillance material has been destroyed or that evidentiary material had been produced pursuant to it, relevant registers, internal organisational materials, and other relevant documents issued by the authorities requesting surveillance, the judges authorising it, or the surveillance authorities. By point 8 of the instruction (as partly amended in April 2019), members of the Bureau and its employees could not be given access to any case file materials which fell outside the strict bounds of the Bureau's competence – that is, materials not among those exhaustively listed in point 7. They could thus not see the entire case files of any preliminary or criminal investigations held by the prosecuting authorities, or assess the materials which had served to support a surveillance application or the results or evidence obtained through surveillance (points 8.1 and 8.2 of the instruction). Any requests by them for access to evidentiary material in the course of an inspection were subject to approval by the competent prosecutor (point 8.3 of the instruction).

(ii) To give instructions and set standards

120. The National Bureau may give binding instructions to the relevant authorities (section 34f(1)(3)). It may also set standards and templates for the relevant registers and for the handling of the relevant materials (section 34f(2) and (3)).

121. According to its annual reports, throughout its existence the National Bureau has given the following number of instructions:

Year	Number of instructions
2014	3
2015	49
2016	3
2017	3
2018	1
2019	7
2020	2

(iii) To bring irregularities to the attention of the competent authorities

122. If the National Bureau finds that special means of surveillance have been used or deployed unlawfully, or that the materials obtained through such means have been stored or destroyed unlawfully, it must bring the matter to the attention of the prosecuting authorities and inform the heads of the relevant requesting and surveillance authorities (section 34f(5) of the 1997 Act).

123. If the National Bureau finds that a judge has unlawfully authorised the use of special means of surveillance, it must bring the matter to the attention of the prosecuting authorities and inform the Supreme Judicial Council and the Minister of Justice (section 34f(6) of the 1997 Act).

(iv) Number of inspections by the National Bureau

124. According to the National Bureau's annual reports, it carried out the following number of inspections each year since 2014:

Year	**Number of inspections**
2014	"more than" 200
2015	242
2016	287
2017	323
2018	133
2019	230
2020	240

3. Parliamentary committee

125. The other body which has the task of supervising the procedures for authorising, deploying and using special means of surveillance, and the storage and destruction of the information obtained by such means, is a standing parliamentary committee – the Parliamentary Committee for Control of the Security Services, of the Application and Use of Special Means of Surveillance, and of Access to the Data under the Electronic Communications Act (section 34h(1) of the 1997 Act, Rule 18 § 1 (4)(a) of the 2017-21 Rules of the National Assembly (superseded by Rule 21 § 7 of the 2021 Rules), and Rule 17 § 1 (9)(a) of the Committee's Rules). The Committee must report to Parliament on those matters each year (Rule 18 § 2 (1) of the 2017-21 Rules of the National Assembly, and Rule 17 § 1 (10)(a) of the Committee's Rules). It has the power to subpoena officials (section 34h(2) of the 1997 Act). It is also involved in the election of the members of the National Bureau (see paragraph 110 above), and supervises the Bureau itself (Rule 5 § 7 of the Committee's Rules).

(a) Manner of election of the Committee's members

126. The Committee has nine members, who come from all parliamentary groups, pro rata the number of their members (Rule 4 of the Committee's Rules).

(b) Powers of the Committee

127. The Committee can (a) examine complaints by individuals and organisations about irregularities in the work of the security services, and (b) refer matters to the prosecuting authorities, if it establishes illegalities as a result of its inspections or on the basis by individual complaints (Rule 17 § 1 (11) and (12) of the Committee's Rules).

128. According to its annual reports, the Committee had received three complaints in 2014, six complaints in 2015, four complaints in 2016, seven complaints in 2017, and four complaints in 2018. Only the report for 2018 made it clear how many of those complaints had related specifically to secret surveillance (the Committee has other competences as well – see paragraphs 205 to 211 below). The Committee's annual reports for 2016, 2017, 2018 and 2019 do not mention any inspections carried out by it. The annual report of the Specialised Criminal Court for 2016 mentions (at p. 2) that in July of that year the Committee had carried out a routine inspection there and had not found any irregularities.

J. Notification of persons placed under secret surveillance

129. The general rule is that all persons who have learned about the use of special means of surveillance must not divulge that information (section 33 of the 1997 Act).

130. The National Bureau must, however, on its own initiative notify individuals who have been placed under secret surveillance unlawfully (section 34g(1) of the 1997 Act). But such notification is not required if (a) it may defeat the purpose of the surveillance, (b) reveal the techniques or equipment used to carry out the surveillance, or (c) entail a risk to the life of an undercover agent or his or her relatives or friends (section 34g(2)). The law does not lay down any requirements about the wording or content of the notification. In a statement drawn up for the purposes of these proceedings, the National Bureau said that according to its internal rules the notification specifies: (a) the number of the surveillance application; (b) the requesting authority; (c) the number of the surveillance warrant; (d) the authority which has issued that warrant; and (e) the period during which there has been unlawful surveillance.

131. In three examples provided by the applicants, and apparently relating to situations under section 34g(2) of the 1997 Act, the notifications by the National Bureau read:

> "The [National Bureau] carried out an inspection pursuant to your complaint no. ..., and came to a decision, and I therefore inform you, pursuant to section 34g(1) of [the 1997 Act], that you have not been subjected unlawfully to special means of surveillance."

132. In one of those cases, it later transpired that there had in fact been surveillance and irregularities in it, on whose basis the relevant court excluded the resulting evidence from the criminal case against the targets of the surveillance (see прис. № 13 от 09.03.2018 г., н. о. х. д. № 727/2015 г., ОС-Хасково, unclear whether final; according to the Government, the appeal proceedings are still pending).

133. In two decisions given in 2016 (unpublished since both cases were classified; copies were provided by the applicants: опр. № 18 от 26.04.2016 г. по адм. д. № С-2/2016 г., ВАС, VII о., and опр. № 28 от 09.06.2016 г. по адм. д. № С-14/2016 г.), the Supreme Administrative Court held that those notifications by the National Bureau were not amenable to judicial review.

134. The 1997 Act does not require the National Bureau to respond to complaints by individuals, but in practice invariably investigates them, and is required to do so under rule 8(1)(9)(a) of its Internal Rules, so long as the complaints are "reasoned".

135. According to the National Bureau's annual reports, it has received the following number of complaints and has made the following number of notifications under section 34g of the 1997 Act:

Year	Complaints	Notifications
2014	27	4
2015	108	10
2016	86	5
2017	133	2 (to the same individual)
2018	110	–
2019	46 (10 of which invalid and not acted on)	2
2020	45 (14 of which invalid and not acted on)	–

K. Civil liability of the authorities for unlawful secret surveillance

136. Section 2(1)(7) of the State and Municipalities Liability for Damage Act 1988, added in March 2009, provides that the State is liable for damage which the investigating and prosecuting authorities or the courts have caused to individuals through the unlawful use of special means of surveillance.

137. Some case-law has already accumulated under that provision.

138. The courts have so far clarified that:

(a) section 2(1)(7) applies only prospectively, for secret surveillance which has taken place after its entry into force (see реш. № 61 от 05.03.2012 г. по гр. д. № 536/2011 г., ВтАС, appeal on points of law not admitted by опр. № 1435 от 15.12.2012 г. по гр. д. № 815/2012 г., ВКС, III г. о.);

(b) a claim for damages under section 2(1)(7) cannot be brought against the court which has issued the surveillance warrant but, as the case may be, against (i) the authority which has applied for the warrant, if it has been issued; (ii) the authority which has deployed special means of surveillance, if no warrant has been applied for or has been refused, or the authority has unlawfully proceeded without a warrant (under the provision of the 1997 Act, section 18, which authorises that in urgent cases – see paragraph 77 above); or (iii) the authority which has used the surveillance materials (see опр. № 3658 от 10.08.2015 г. по гр. д. № 126/2015 г., ОС-Благоевград, upheld by опр. № 2987 от 28.10.2015 г. по в. ч. гр. д. № 3999/2015 г., САС, appeal on points of law not admitted by опр. № 89 от 01.04.2016 г. по ч. гр. д. № 240/2016 г., ВКС, I г. о.; опр. № 240 от 28.03.2016 г. по в. ч. гр. д. № 171/2016 г., ОС-Перник, appeal on points of law not admitted by опр. № 344 от 19.09.2016 г. по ч. гр. д. № 3228/2016 г., ВКС, III г. о.; опр. от 06.01.2017 г. по гр. д. № 5567/2016 г., СГС, upheld by опр. № 1284 от 12.04.2017 г. по в. ч. гр. д. № 1349/2017 г., САС, appeal on points of law not admitted by опр. № 303 от 22.08.2017 г. по ч. гр. д. № 2731/2017 г., ВКС, III г. о.; and реш. № 203 от 27.02.2019 г. по гр. д. № 5061/2017 г., ВКС, III г. о.);

(c) it is for the claimant to specify, in the statement of claim, which authority has used special means of surveillance with respect to him or her, and to direct the claim against that authority (see опр. № 778 от 06.03.2018 г. по в. гр. д. № 1063/2018 г., САС, unclear whether final);

(d) a civil court dealing with a claim for damages under section 2(1)(7) can rely on the National Bureau's findings of fact but is not bound by the Bureau's assessment of whether the surveillance was unlawful (see № 166 от 03.08.2018 г. по гр. д. № 4454/2017 г., ВКС, IV г. о.);

(e) the mere authorisation to use special means of surveillance can be grounds for liability under section 2(1)(7); their subsequent deployment goes only to the quantum of damages (see № 166 от 03.08.2018 г. по гр. д. № 4454/2017 г., ВКС, IV г. о.);

(f) liability under section 2(1)(7) can arise if the surveillance warrant has been issued in relation to an offence which by law cannot be prevented or investigated through such means, or the application for a warrant has been made by an incompetent authority or was incomplete, but not if the application has been duly made, since the civil courts dealing with claims for damages under that provision cannot gainsay whether the judges who

have issued a surveillance warrant have correctly assessed the need for surveillance on the facts (ibid., and реш. № 203 от 27.02.2019 г. по гр. д. № 5061/2017 г., ВКС, III г. о.);

(g) failure to comply with the rules governing the timely destruction of surveillance information (see paragraphs 94 and 95 above) is not in itself grounds for liability under section 2(1)(7) (see реш. № 6303 от 10.10.2018 г. по гр. д. № 11689/2016 г., СГС (final), rectified with реш. № 3 от 02.01.2019 г. по гр. д. № 11689/2016 г., СГС); and

(h) the limitation period for bringing a claim under section 2(1)(7) (five years – section 110 of the Obligations and Contracts Act 1950; see also *Harizanov v. Bulgaria* (dec.), no. 53626/14, § 52, 5 December 2017) starts to run when the person concerned is notified by the National Bureau that he or she has been placed under surveillance unlawfully (see paragraph 130 above), because without such notification that person had no means of vindicating his or her rights (see реш. № 166 от 03.08.2018 г. по гр. д. № 4454/2017 г., ВКС, IV г. о.).

139. The only form of relief available in proceedings under the 1988 Act is money damages (sections 4(1) and 8(1)). In cases under section 2(1)(7), the courts have so far awarded damages ranging from 2,000 to 27,000 Bulgarian levs (BGN) (1,023 to 13,805 euros (EUR)) in respect of various instances of unlawful use of special means of surveillance:

(a) use of such means in relation to offences in respect of which this is not authorised by the law and in the absence of sufficient factual justification in the surveillance application (see реш. № 1811 от 21.07.2017 г. по в. гр. д. № 615/2017 г., САС, upheld by реш. № 166 от 03.08.2018 г. по гр. д. № 4454/2017 г., ВКС, IV г. о., and реш. № 1960 от 30.07.2019 г. по гр. д. № 2052/2018 г., САС, appeal on points of law not admitted by опр. № 424 от 15.05.2020 г. по гр. д. № 4684/2019 г., ВКС, III г. о.);

(b) obtaining a warrant for renewed surveillance without fresh justification and surveillance beyond the time-limits (see реш. № 2808 от 04.05.2018 г. по гр. д. № 11366/2016 г., СГС, upheld by реш. № 1034 от 01.05.2019 г. по в. гр. д. № 5808/2018 г., САС, unclear whether final);

(c) obtaining a surveillance warrant from an incompetent judge and without providing sufficient justification in the surveillance application (see реш. № 12538 от 22.12.2020 г. по в. гр. д. № 1690/2020 г., САС, appeal on points of law not admitted by опр. № 60753 от 04.11.2021 г. по гр. д. № 1845/2021 г., ВКС, III г. о.);

(d) obtaining a surveillance warrant from an incompetent judge and surveillance outside the relevant time-limit (see реш. № 312 от 16.10.2020 г. по гр. д. № 238/2020 г., ОС-Бургас, upheld by реш. № 13 от 19.02.2021 г. по в. гр. д. № 474/2020 г., АС-Бургас, appeal on points of law not admitted by опр. № 60653 от 12.10.2021 г. по

гр. д. № 1872/2021 г., ВКС, IV г. о.), and реш. № 262304 от 07.04.2021 г. по гр. д. № 8701/2019 г., СГС, unclear whether final);

(e) obtaining a surveillance warrant without providing enough factual data in the initial application (and in a renewal application) and without having enough information that the person sought to be placed under the surveillance could in fact be suspected of an offence (see реш. № 6303 от 10.10.2018 г. по гр. д. № 11689/2016 г., СГС (final), rectified with реш. № 3 от 02.01.2019 г. по гр. д. № 11689/2016 г., СГС);

(f) obtaining a surveillance warrant solely on the basis of an anonymous signal and without detailing the previous, if any, steps in the investigation (see реш. № 7225 от 20.11.2018 г. по в. гр. д. № 16408/2017 г., СГС (final), overturning реш. № 192358 от 11.08.2017 г., по гр. д. № 13365/2016 г., СРС);

(g) surveillance outside the relevant time-limit (see реш. № 8690 от 21.12.2017 г. по гр. д. № 6213/2017 г., СГС, upheld by реш. № 1536 от 01.06.2018 г. по в. гр. д. № 1509/2018 г., САС, upheld by реш. № 293 от 17.03.2020 г. по гр. д. № 3963/2018 г., ВКС, IV г. о.).

(h) surveillance for the purpose of tracing a fugitive, that not being among the situations envisaged under the 1997 Act (see реш. № 1360 от 12.01.2017 г. по гр. д. № 781/2015 г., РС-Перник, upheld by реш. № 173 от 23.06.2017 г. по в. гр. д. № 237/2017 г., ОС-Перник, upheld, with an increase of the award of damages, by реш. № 203 от 27.02.2019 г. по гр. д. № 5061/2017 г., ВКС, III г. о.).

140. In all those cases, the claimants had been notified by the National Bureau that they had been subjected to unlawful surveillance, and the courts had before them information from the Bureau, and in some cases also surveillance materials adduced as evidence in criminal proceedings against the people concerned. In its annual report for 2016, the Bureau said (at p. 25) that it had provided the civil courts with materials from its inspections pursuant to requests made by them in such cases.

141. In a March 2018 decision, the Sofia Court of Appeal held, among other things, that under the general rule of *affirmanti incumbit probatio*, in proceedings under section 2(1)(7) of the 1988 Act the burden was on claimants to show which authority had used special means of surveillance unlawfully with respect to them, and was thus a proper defendant to their claim (see опр. № 778 от 06.03.2018 г. по в. гр. д. № 1063/2018 г., САС, unclear whether final).

142. In a recent case in which the use of special means of surveillance was not apparent from the materials in the criminal proceedings against the claimant, the courts dismissed the claim under section 2(1)(7) of the 1988 Act as unproven, noting that it was for the claimant to make out her assertion that such means had been used with respect to her (see реш. от 31.12.2019 г. по гр. д. 31075/2015 г., СРС, upheld by реш. № 260651 от

29.01.2021 г. по в. гр. д. № 6434/2020 г., СГС, appeal on points of law apparently pending).

143. In a June 2020 decision, the Burgas Regional Court held that a claim under section 2(1)(7) of the 1988 Act could be brought only if the use of special means of surveillance with respect to the claimant was apparent either from the materials adduced as evidence in a criminal case or from a notification by the National Bureau (see опр. № 1786 от 26.06.2020 г. по гр. д. № 1037/2020 г., ОС-Бургас, apparently final).

144. In an April 2021 judgment, the Sofia City Court held that since the National Bureau, when notifying the claimant, had not given an account of the content of the surveillance applications or the surveillance warrants, there was no basis on which to find that the use of special means of surveillance had been unlawful. The court hence dismissed the claim (see реш. № 262304 от 07.04.2021 г. по гр. д. № 8701/2019 г., СГС, unclear whether final).

L. Criminal liability of officials for unlawful secret surveillance

145. By Article 284c of the Criminal Code, added in 2009, it is an offence for an official unlawfully to authorise or order the use of special means of surveillance, or use them, or store information acquired through them. There has so far been only one reported conviction under that provision (see paragraph 56 above).

II. DISCLOSURE OF DOCUMENTS IN CIVIL PROCEEDINGS

146. Article 190 § 1 of the Code of Civil Procedure provides that a party may ask the court to order the opposing party to disclose a document held by it, if it explains to the court why that document is relevant for its case. If the opposing party fails to disclose the document, the court may draw adverse inferences (Article 190 § 2 read in conjunction with Article 161). The opposing party may refuse to disclose a document if (a) its contents relate to its private or family life, or (b) its disclosure would bring that party or its relatives into disrepute or trigger a criminal prosecution against them (Article 191 § 1). If those considerations apply only to a part of the document, the opposing party may be ordered to present an excerpt (Article 191 § 2).

147. Article 192 § 1 of the Code provides that a party may ask the court to order a third party to present a document in its possession. If that third party does not present the document without justification, it may be fined by the court, and is liable towards the party which has requested the document for any damage resulting from its non-presentation (Article 192 § 3).

148. According to a leading practical treatise on civil procedure, a party's request for the disclosure of a document under Articles 190 or 192

must, as far as practicable, spell out its type, date, author and other distinguishing features. It is furthermore impermissible to require the opposing party or a third party to create, for the purposes of the proceedings, a document which does not already exist (see *Граждански процесуален кодекс*, *Приложен коментар*, ИК „Труд и право“, 2017 г., p. 318).

149. Article 186 of the same Code provides that a court hearing a civil case may request a public authority to provide official documents or give the party which intends to rely on those documents a judicial certificate which that party can present to the relevant public authority with a view to obtaining those documents. The relevant public authority is bound to either issue those documents or explain the reasons why it cannot do so.

150. It does not appear that there are any reported decisions under Articles 186, 190 or 192 of the Code of Civil Procedure in relation to cases under section 2(1)(7) of the 1988 Act (see paragraphs 136 to 144 above).

III. RETENTION AND ACCESSING OF COMMUNICATIONS DATA

A. General evolution of the legal regime

151. The regime for retention and subsequent accessing of communications data for law-enforcement purposes was introduced when section 251 of the Electronic Communications Act 2007 came into force in May 2007, and when the Minister of Internal Affairs and the head of the State Agency for Information Technologies and Communications issued, based on a statutory delegation in section 251(2), Regulations no. 40 of 7 January 2008 “on the categories of data and the manner in which it is to be retained and made available by enterprises offering public communications networks or services for national-security purposes and the detection of offences”.

152. Those provisions were put in place to transpose the so-called Data Retention Directive (see paragraph 232 below) (paragraph 4 of the Regulations’ transitional and concluding provisions).

153. Regulation 5 of Regulations no. 40 of 2008 was quashed by the Supreme Administrative Court in December 2008 following a challenge by the fourth applicant, the Access to Information Foundation (see реш. № 13627 от 11.12.2008 г. на ВАС по адм. д. № 11799/2008 г., ВАС, петчл. с-в, ДВ, бр. 108/2008 г.).

154. With effect from March 2009, Parliament amended section 251 of the 2007 Act, removing the statutory delegation enabling the issuing of regulations pursuant to it. The status of Regulations no. 40 of 7 January 2008, which have not been formally repealed, is thus unclear.

155. In early 2010 Parliament added new sections 250a-250f, 251a, 261a-261b, 327(4)-(7), and 332a to the 2007 Act, and amended section 251.

This was again done with a view to transposing the Data Retention Directive (paragraph 10 of the additional provisions of the February 2010 Act for the amendment of the 2007 Act).

156. Following a legal challenge brought by the Ombudsman of the Republic in April 2014, in the wake of the judgment of the Court of Justice of the European Union ("CJEU") holding the Data Retention Directive invalid (see paragraph 233 below), in mid-March 2015 the Constitutional Court declared sections 250a-250f, 251 and 251a of the 2007 Act unconstitutional as a whole (see реш. № 2 от 12.03.2015 г. по к. д. № 8/2014 г., КС, обн., ДВ, бр. 23/2015 г.).

157. In reaction to that judgment, in late March 2015 Parliament added new sections 251b-251i to the 2007 Act, and a new Article 159a to the Code of Criminal Procedure. They have been amended several times since then. In 2016, a new section 251d[1] was added.

158. In March 2020, following the outbreak of the COVID-19 pandemic, Parliament amended sections 251b(2), 251c(2), 251d(5) and 251d[1](1), (3) and (4) of the 2007 Act to make it possible to use retained location (cell ID) data to enforce quarantine and isolation measures for people who are ill with or are carriers of a number of contagious diseases, including COVID-19.

159. In November 2020 the Constitutional Court declared the amendment unconstitutional as a whole (see реш. № 15 от 17.11.2020 г. по к. д. № 4/2020 г., КС, обн., ДВ, бр. 101/2020 г.). It held, with reference to, among other things, the CJEU's case-law in that domain (see paragraphs 233 and 240 to 243 below), that resorting to the general retention of location (cell ID) data for six months and the consequent possibility for the authorities to access it to enforce measures intended to prevent the spread of infectious diseases disproportionately interfered with the constitutional right to privacy.

B. The regime as it stands at present

160. All legal provisions cited below are set out as they stood on 7 December 2021.

1. Types of communications data subject to retention

161. All electronic communications service providers in Bulgaria must retain, for six months, the following types of communications data for all of their users: (a) data necessary to trace and identify the source of a communication; (b) data necessary to identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication; (d) data necessary to identify the type of a communication; (e) data necessary to identify the user's communication equipment or what purports to be that equipment; and (f) the cell ID for

mobile communication equipment (section 251b(1) of the 2007 Act). Section 251i defines in detail what each of those types of data consist of for fixed and mobile telephony, and Internet access, email and Internet telephony. Those provisions reproduce nearly verbatim the wording of Article 5 of the Data Retention Directive (see paragraph 232 below). Communications service providers which fail to comply with this data-retention obligation are liable to a pecuniary sanction ranging from BGN 3,000 to BGN 25,000 (section 327(4) of the 2007 Act).

162. According to the annual reports of the Commission for Protection of Personal Data (see paragraphs 198 to 203 below), the overall number of communications service providers in Bulgaria and the number of such providers reporting to the Commission about data retention each year since 2015[16] was as follows:

Year	Overall number of communications service providers	Communications service providers reporting to the Commission
2015	1,160	77[17]
2016	1,143	104
2017	not specified	93
2018	not specified	117
2019	not specified	99

2. Purposes for which that data is retained

163. Such data is retained for (a) national-security purposes; (b) the prevention, detection or investigation of "serious" criminal offences[18] (including, following a January 2018 amendment, the prevention of "serious offences" of corruption by a special commission); (c) the tracing of people who have been finally sentenced to imprisonment with respect to a serious criminal offence or who have fallen or could fall in a situation which puts their life or health at risk; and (d) (this applies solely to cell ID) the carrying out of search-and-rescue operations with respect to people in distress (section 251b(2) of the 2007 Act and Article 159 § 2 of the Code of Criminal Procedure).

[16] The Commission's annual report for 2021, which should contain the statistics for 2020, has not been published yet.

[17] In its annual report for 2015, the Commission surmised (at p. 91) that the low number of communications service providers reporting to it about data retention was probably due to the providers' interpreting the law as requiring them to report only if they had received an access request by the authorities during the reporting period.

[18] For the definition of a "serious" criminal offence under Bulgarian law, see paragraph 18 above.

3. Rules on the processing of the retained data by the communications service providers

164. The retained data must be processed and kept by the communications service providers in line with the rules on the protection of personal data (section 251b(4) of the 2007 Act).

165. Communications service providers must ensure that the retained data is: (a) of the same quality and subject to the same security and protection as the data on their networks; (b) subject to appropriate technical and organisational measures to protect it against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure; (c) subject to appropriate technical and organisational measures to ensure that it can be accessed by specially authorised personnel only; and (d) destroyed at the end of the period of retention, except as specifically provided for by law (section 261a(2) of the 2007 Act).

4. Destruction of retained data which has not been accessed by the authorities

166. Communications service providers must destroy the retained data immediately after the expiry of the six-month time-limit for its retention, and send a record attesting that destruction to the Commission for Protection of Personal Data (see paragraphs 198 to 203 below) not later than the fifth day of the respective month (section 251g(1) of the 2007 Act). The Commission can control whether that duty has been complied with (see paragraph 204 (b) below).

5. Authorisation procedure

(a) Authorities entitled to seek access

167. Only a limited number of authorities may seek access to the retained data, within the spheres of their respective competencies.

168. Outside the framework of already pending criminal proceedings, such access may be sought only by: (a) the specialised directorates and the territorial directorates and units of the State Agency for National Security; (b) various directorates of the Ministry of Internal Affairs (national police, fight against organised crime, border police, internal affairs, and the regional directorates); (c) the military-intelligence and military-police services attached to the Minister of Defence; (d) the Intelligence Agency; (e) the specialised anti-corruption directorate;[19] and (f) (as regards cell ID data needed for search-and-rescue operations – see paragraphs 161 (f) and 163 (d) above) the Fire Safety and Civil Protection Directorate of the Ministry of Internal Affairs, including its territorial units (section 251c(1)

[19] See footnote 3 above.

and (2) of the 2007 Act). If access is sought by a foreign authority, the request must be made through a central or specialised directorate of the State Agency for National Security or the Ministry of Internal Affairs (section 251h(2)).

169. In the course of criminal proceedings, access may sought by the court hearing the case (if it is already at the trial or appeal stages) or by the public prosecutor in charge of supervising the pre-trial investigation (Article 159a § 1 of the Code of Criminal Procedure).

170. According to the annual reports of the parliamentary committee overseeing the system (see paragraphs 205 to 211 below), the number of access applications per year in 2015-19 was as follows:

Year	Access applications outside criminal proceedings	Access applications by public prosecutors
2015	12,948	13,354
2016	15,805	24,758
2017	13,233	25,252
2018	10,603	22,563
2019	13,108	18,883

(b) Content of the access application

171. Access applications made outside the context of pending criminal proceedings must be reasoned and set out (a) the legal grounds and the purpose for which access is being sought; (b) the number of the case file in connection with which access is being sought; (c) if available, information about the user(s) whose data is being sought; (d) the data which must be provided; (e) the period of time with respect to which data is being sought, which must be "reasonable" and "necessary to attain the purpose" for which the access application is being made; (f) a full account of the circumstances which show that the data is needed for a relevant purpose; and (g) the official to whom the data must be made available (section 251c(3) of the 2007 Act).

172. Access applications made by a public prosecutor in the course of criminal proceedings must likewise be reasoned and set out (a) information about the alleged offence in connection with which access is being sought; (b) a description of the circumstances underlying the access application; (c) information about the user(s) whose data is being sought; (d) the "reasonable" period of time with respect to which data is being sought; and (e) the investigating authority to which the data must be made available (Article 159a § 3 of the Code of Criminal Procedure).

(c) Authorities competent to issue access warrants

173. Outside the framework of already pending criminal proceedings, the warrant may be issued by the president of the district court which is territorially competent with respect to the place where the requesting authority is located, or a judge to whom its president has delegated that power (section 251d(1) of the 2007 Act).

174. If the access application concerns alleged terrorist offences (including preparatory ones), the warrant may be issued only by the President of the Specialised Criminal Court or a judge to whom he or she has delegated that power (section 251d(2) of the 2007 Act).

175. If the access application has been made at the request of a foreign authority, the warrant must be issued by the Sofia City Court or a judge to whom he or she had delegated that power (section 251h(2) of the 2007 Act).

176. Special rules govern the accessing of retained communications data relating to district court presidents or their relatives, or the President of the Specialised Criminal Court or his or her relatives (except if access to the data is being sought for a search-and-rescue operation): in those cases the warrant may be issued by, respectively, the respective regional court president or the President of the Specialised Criminal Court of Appeal (section 251d(4) of the 2007 Act).

177. If the access application has been made by a public prosecutor in the course of criminal proceedings, the warrant may be issued by a judge of the competent first-instance court (Article 159a § 1 of the Code of Criminal Procedure).

(d) Manner of examination of access applications

178. When access is sought in connection with an alleged terrorist offence, the access warrant must be issued within twenty-four hours of the receipt of the access application (section 251d(3) of the 2007 Act). Neither the 2007 Act nor Article 159a of the Code of Criminal Procedure lay down express time-limits for the examination of access applications in other cases.

179. When relating to an access application made outside the framework of already pending criminal proceedings, the decision to issue a warrant must be reasoned, and the warrant must set out (a) the data which must be provided; (b) the period of time with respect to which data is to be provided, which must be "reasonable" and "necessary to attain the purpose" for which the access application has been made; and (c) the official to whom the data is to be made available (section 251d(6) of the 2007 Act).

180. When relating to an access application made in the course of criminal proceedings, the decision to issue a warrant must likewise be reasoned and set out (a) the data which must be provided; (b) the period of time with respect to which data is to be provided, which must be "reasonable"; and (c) the investigating authority to which the data is to be

made available (Article 159a §§ 1 and 4 of the Code of Criminal Procedure).

181. All district courts, the Specialised Criminal Court and the Sofia City Court must record their decisions to allow or refuse access applications in non-public registers (sections 251d(7) and 251h(2) *in fine* of the 2007 Act).

182. According to the annual reports of the parliamentary committee overseeing the system (see paragraph 205 to 211 below), the judicial decisions to allow or refuse access application each year in 2015-19 were as follows:

Year	Access warrants issued	Access applications refused
2015	25,303[20]	2,911
2016	39,990	3,479
2017	38,492	2,762
2018	33,835	2,287
2019	29,325	2,666

(e) Retrospective authorisation in urgent cases

183. In cases of an immediate danger of the commission of a terrorist offence (including a preparatory one), access may be provided without a prior judicial warrant (section 251d[1](1) of the 2007 Act). In those cases, the (direct) access request must set out (a) the legal ground for access; (b) the data which is to be made available; (c) the period of time with respect to which data is to be provided, which must be "reasonable"; and (d) the official to whom the data is to be made available (section 251d[1](2)).

184. The head of the requesting authority must then immediately inform the relevant judge of the access, send him or her the access request, and explain the reasons why direct access had been necessary. Those reasons must include a full account of the circumstances which caused the authority to think that a terrorist offence was imminent (section 251d[1](3) of the 2007 Act).

185. If the judge does not approve the access request within twenty-four hours, any data made available pursuant to the direct access request must be destroyed by the authority which has received them, and the communications service provider must be informed of that (section 251d[1](4) of the 2007 Act). If the judge approves the access request, that validates all steps already taken with respect to it (section 251d[1](5)).

[20] The sum of the number of access warrants and of decisions to refuse access applications each year is greater than the annual number of applications (see the table under paragraph 170 above) because if an access application concerns data retained by several communications service providers, some courts issue a separate access warrant with respect to each of those providers.

186. The annual report of the parliamentary committee overseeing the system (see paragraphs 205 to 211 below) for 2019 – the only one which mentioned the point – said (at p. 11), that during that year the courts had approved 317 such direct access requests made in urgent cases.

6. Procedure for accessing retained data

187. Communications service providers must arrange for the possibility to receive access requests, including direct access requests, round the clock (section 251e(1) of the 2007 Act). They must keep the relevant authorities apprised of their access correspondents (section 251e(1)). Failure to do so may result in a pecuniary sanction ranging from BGN 2,000 to BGN 12,000 (section 327(5)).

188. In regular cases, the communications service providers must provide the data as quickly as possible and in any event within seventy-two hours of receiving the access request. However, the Minister of Internal Affairs or the head of the State Agency for National Security, or their duly authorised deputies, may fix a shorter time-limit in a given case. In cases concerning alleged terrorist offences, the data must be provided immediately (section 251f(2) of the 2007 Act). Failure to do so may result in a pecuniary sanction ranging from BGN 10,000 to BGN 25,000, and from BGN 15,000 to BGN 50,000 in repeat cases (section 327(6) and (7)). When it comes to search-and-rescue operations, access must be provided immediately and in any event not later than two hours of receipt of the access request; if the life or health of the people concerned are at serious risk, the Minister of Internal Affairs or a duly authorised official may fix a shorter time (section 251f(3)).

189. All access requests must be recorded by the communications service providers in a special non-public register (section 251f(1) *in fine* of the 2007 Act). Only duly authorised employees may deal with access requests (section 251f(4)). The document setting out the data sought by the authorities must be signed by the head of the communications service provider or a duly authorised employee, likewise recorded in a special register, and sent directly to the designated official (section 251f(5)).

190. If technically feasible, all those exchanges of documents between the authorities and communications service providers must be done electronically (section 251f(6) of the 2007 Act).

191. If requested by the relevant authority and authorised by the relevant judge, retained data which has been accessed by it may be kept by the communications service provider for a maximum of three months of the date on which it was accessed (section 251f(7) of the 2007 Act).

192. According to the annual reports of the Commission for Protection of Personal Data (see paragraphs 198 to 203 below), the number of instances in which retained communications data had been provided to the

authorities and the number of access requests not met each year since 2010[21] was as follows:

Year	Instances of access provided	Access requests not met
2010	38,861	920
2011	74,296	1,376
2012	91,159	1,083
2013	96,652	1,606
2014	107,769	705
2015	70,543	2,783
2016	64,959	546
2017	65,073	347
2018	56,527	416
2019	47,553	291

7. Storage of retained data accessed by the authorities

193. Neither the 2007 Act nor the Code of Criminal Procedure contain provisions spelling out how retained communications data accessed by the authorities is to be stored by them. A perusal of judicial decisions mentioning such data suggests that when used in the course of criminal proceedings, it is kept in the case file of the respective case (see, for instance, прис. № 4 от 19.01.2018 г. по н. о. х. д. № 234/2017 г., ОС-Хасково; прис. № 32 от 10.09.2019 г. по н. о. х. д. № 475/2018 г., ОС-Стара Загора; and прис. № 34 от 11.12.2019 г. по н. о. х. д. № 650/2019 г., ОС-София). Neither the Rules on the administrative services of the courts, issued by the Supreme Judicial Council in 2017, nor the Rules on the administrative services of the prosecutor's offices, issued by the Supreme Judicial Council in 2013, which govern the storage of case files by, respectively, the courts and the prosecuting authorities, contain special rules on the storage of communications data featuring in a case file.

8. Destruction of retained data accessed by the authorities

194. If they do not use it to open criminal proceedings, the authorities must destroy the communications data which they have accessed within three months of receiving it. The destruction is to be done by a three-member commission appointed by the head of the respective authority. The commission must draw up a record attesting the destruction and send it immediately to the judge who has issued the access warrant. That record

[21] The Commission's annual report for 2021, which should contain the statistics for 2020, has not been published yet.

must be registered in the warrants register kept by the respective court (see paragraph 181 above) (section 251g(2) of the 2007 Act).

195. If the competent judge does not validate retrospectively access to the retained data accessed by the authorities without a prior warrant under the urgent procedure (see paragraphs 183 to 185 above), that data must be destroyed immediately in the same way (section 251g(3) of the 2007 Act).

196. Communications data accessed in the course of criminal proceedings which turns out to be irrelevant or unhelpful for establishing the facts of the case must likewise be destroyed. That is done on the basis of an order of the judge who has issued the access warrant (made on a proposal by the public prosecutor in charge of the case), in accordance with rules laid down by the Chief Prosecutor (those rules do not appear to be publicly available). Within seven days of the destruction, the communications service providers and the public prosecutor in charge of the case must send records attesting the destruction to the judge who has issued the access warrant (Article 159a § 6 of the Code of Criminal Procedure).

9. Authorities supervising the retention of and the access to communications data

(a) Judges who have issued the respective access warrants

197. As noted in paragraphs 194, 195 and 196 *in fine* above, the judge who has issued the access warrant must be informed of the destruction of any irrelevant or unhelpful communications data by the relevant law-enforcement authority.

(b) Commission for Protection of Personal Data

198. The Commission for Protection of Personal Data oversees the retention of communications data for law-enforcement purposes by the communications service providers (section 261a(1) and (2) of the 2007 Act). By section 262 of the 2007 Act, as amended in February 2019, the Commission's supervision of the processing of personal data caused by the retention and accessing of communications data must be carried out in line with the requirements of the General Data Protection Regulation ("GDPR" – see paragraphs 234 to 237 below) and the Protection of Personal Data Act 2002 (see paragraphs 218 and 225 below).

199. The same Commission is also generally competent to oversee the processing of personal data by non-judicial authorities for law-enforcement purposes (see paragraph 225 below).

(i) Manner of election and term of office of the Commission's members

200. The Commission, which is an "independent supervisory authority", consists of a chairperson and four members, all elected by Parliament following a proposal by the Council of Ministers for a term of five years,

renewable once (sections 6(1) and 7(1) and (2) of the Protection of Personal Data Act 2002). They must have university education in computer science, information technology or law (section 8(1)(1)). The chairperson must be a qualified lawyer (section 8(3)). Parliament may terminate their term of office prematurely only in a limited number of situations: criminal conviction, grave misconduct, incapacity to carry out their duties for more than six months, or duly established conflict of interests (section 8(4)(2)).

(ii) Powers of the Commission under the 2007 Act

(α) To obtain information

201. The Commission may request communications service providers to provide it with any information relevant to its mandate in that domain (section 261a(3)(1) of the 2007 Act). Communications service providers must also provide it annually with statistical information about (a) the number of cases in which the authorities have accessed retained communications data, (b) the time elapsed between the date on which the data were retained and the date on which the competent authority requested access to it, and (c) the number of cases in which access requests have been impossible to meet (section 261a(4)). The Commission must report that statistical information annually to Parliament and to the European Commission[22] (section 261a(5)).

202. The Commission may also check how communications service providers comply with their duties to communicate personal data breaches to users (see paragraph 214 below) (section 261d(2) of the 2007 Act), and inspect the technical and organisational measures taken by communications service providers for storing retained communications data (section 261d(3)).

(β) To give instructions and recommendations

203. The Commission may give binding instructions, which must be complied with immediately (section 261a(3)(2) of the 2007 Act). Those instructions may in particular be on when and how communications service providers must communicate personal data breaches to affected persons (section 261d(1)). It may also recommend best practices on the level of security when storing retained communications data (section 261d(3) *in fine*).

(γ) To impose sanctions

204. The Commission may sanction communications service providers who have not complied with their duties to (a) communicate a personal data

[22] The requirement to report to the European Commission appears to be a vestige of Article 10 § 1 of the Data Retention Directive (see paragraph 232 below).

breach to the persons affected by it (see paragraph 214 below) or (b) destroy retained communications data within the statutory time-limit (see paragraph 166 above) (sections 261d(2) *in fine* and 323a of the 2007 Act).

(c) Parliamentary committee

205. The same standing parliamentary committee which is in charge of overseeing secret surveillance – the Parliamentary Committee for Control of the Security Services, of the Application and Use of Special Means of Surveillance, and of Access to the Data under the Electronic Communications Act (see paragraph 125 above) – is also tasked with overseeing the retention and accessing of communications data. It oversees not only communications service providers but also the authorities entitled to access the data and the procedures whereby they seek and obtain access to it, and must ensure that individual rights and freedoms are protected against unlawful access (section 261b(1) of the 2007 Act, and Rule 18 §§ 1(4)(b) and 2(2) of the 2017-21 Rules of the National Assembly). The Committee must report each year about any inspections which it has carried out (section 261b(2)(4)).

(i) Manner of election of the Committee's members

206. This is set out in paragraph 126 above.

(ii) Powers of the Committee under the 2007 Act

(α) To obtain information

207. The Committee may: (a) request communications service providers, the authorities entitled to access retained data (see paragraphs 168 and 169 above) and the Commission for Protection of Personal Data to provide it with any information relevant to its mandate; (b) check the way in which retained data, access applications and access warrants are being kept, and the way in which retained data is being destroyed; and (c) access the premises of relevant authorities or communications service providers (section 261b(2)(1) to (2)(3) of the 2007 Act). The Ministry of Internal Affairs, the State Agency for National Security, the Intelligence Agency and the Chief Prosecutor must provide the Committee statistics about the annual number of access requests, access warrants, and instances of accessing and destruction of data (section 261b(3)).

208. In its annual report for 2017, the Committee noted that experts employed by it had carried out 302 inspections in courts and law-enforcement authorities. Those inspections had revealed (a) diverging practices in the courts in relation to access requests, and (b) a failure on the part of the public prosecutors in charge of the respective criminal cases to comply with their duty under Article 159a § 6 of the Code of Criminal Procedure to propose to the competent judges to order the destruction of

accessed communications data which had turned out to be irrelevant or unhelpful (see paragraph 196 above). The report also noted various instances in which the legal requirements for access had not been complied with.

209. In its annual report for 2018, the Committee noted that experts employed by it had carried out 229 inspections, and had again seen various diverging practices, as well as failures by the prosecuting authorities to destroy irrelevant communications data on the basis that that data might turn out to be helpful at a later stage of the investigation. The report again noted various instances in which the legal requirements for access had not been complied with.

210. In its annual report for 2019, the Committee noted that experts employed by it had carried out 136 inspections, and had once again seen various diverging practices, as well as failures by the prosecuting authorities to propose to the competent judges to order the destruction of irrelevant communications data (see paragraph 208 (b) above). The report again noted various instances in which the legal requirements for access had not been complied with.

(β) To give instructions

211. The Committee may give instructions designed to improve the procedures for processing and destruction of the retained data (section 261b(2)(4) *in fine* of the 2007 Act).

(iii) To bring irregularities to the attention of the competent authorities

212. If the Committee finds that retained communications data has been used, stored or destroyed unlawfully, it must bring the matter to the attention of the prosecuting authorities, and inform the heads of the relevant access-requesting authorities and communications service providers. Those heads must report back to the Committee on the steps taken to remedy those irregularities (section 261b(4) of the 2007 Act).

10. Notification arrangements

(a) In cases of unlawful access or attempted access

213. If the Committee finds that someone's retained communications data has been accessed or sought to be accessed unlawfully, it must notify that individual (section 261b(5) of the 2007 Act). Such notification is not required if it would risk defeating the purpose(s) under section 251b(2) of the 2007 Act for which the data has been accessed or sought to be accessed (see paragraph 163 above).

(b) In cases of a personal data breach

214. If a communications service provider becomes aware of a personal data breach, it must inform the Commission for Protection of Personal Data within three days (section 261c(1) the 2007 Act). If the breach can affect negatively the personal data or the private life of a user or another person, the provider must communicate it to them (section 261c(2)), but may omit doing so if it satisfies the Commission that it has put in place appropriate technical and organisational protection measures in relation to the personal data affected by the breach – such as technical measures making the data unintelligible to anyone not authorised to access it (section 261c(3)). If the provider has not itself communicated the breach, the Commission, having reviewed its potential negative consequences, may nevertheless require the provider to communicate the breach to the affected persons (section 261c(4)). Section 261c(5) sets out the minimum content of the communication.

IV. RELEVANT DATA PROTECTION PROVISIONS

215. All legal provisions cited below, which came into force in February 2019, are set out as they stood on 7 December 2021.

A. Field of application

216. The provisions of the Protection of Personal Data Act 2002 apply only to individuals (natural persons), regardless of whether they concern the processing of personal data falling under the GDPR (see paragraph 234 below) or the processing of such data by the authorities for law-enforcement purposes (section 1(1) and (2)). They do not apply to processing of such data for defence or national security purposes either, unless expressly provided elsewhere (section 1(5)).

B. On the processing of personal data by private persons

1. Limitations on the rights of data subjects

217. A controller or processor of personal data may restrict, wholly or in part, the access, rectification, erasure and other rights of the data subject, as laid down in Articles 12 to 22 of the GDPR, or eschew the duty under Article 34 of the GDPR to communicate a personal data breach to the data subject, if the exercise of those rights or the performance of that duty would create a risk for, among others, (a) national security, (b) public security, or (c) the prevention, investigation, detection or prosecution of criminal offences (section 37a(1) of the Protection of Personal Data Act 2002, which echoes Article 23 § 1 of the GDPR – see paragraph 234 below).

2. Remedies

218. Data subjects considering that their rights under the GDPR or the 2002 Act have been breached may complain to the Commission for Protection of Personal Data, and seek judicial review of its decision (section 38(1) and (7) of the 2002 Act, which echoes Article 77 § 1 and Article 78 §§ 1 and 2 of the GDPR – see paragraph 236 below). Data subjects may also seek judicial review of the actions or decisions of the data controller or processor, or damages from them, in case they have processed their personal data unlawfully (section 39(1) and (2) of the 2002 Act, which echoes Articles 79 § 1 and 82 § 1 of the GDPR – see paragraphs 237 and 238 below).

C. On the processing of personal data by the competent authoritiesfor law-enforcement purposes

1. Conditions on which such processing is lawful

219. Processing of personal data by the competent law-enforcement authorities is lawful if it is (a) necessary for the prevention, investigation, detection or prosecution of a criminal offence and is (b) based on a statute or statutory instrument or on a provision of European Union law specifying the purposes of the processing and the categories of personal data to be processed (section 49 of the 2002 Act, transposing Article 8 of Directive (EU) 2016/680 – see paragraph 239 below). Such data must, among other things, (a) be processed in a manner ensuring its appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, (b) not be processed in a manner incompatible with the explicit legitimate purposes for which it has been collected, and (c) kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which they are processed (section 45(1)(2), (1)(5) and (1)(6), transposing Article 4 § 1 (b), (e) and (f) of the Directive).

2. Possible limitations on the rights of data subjects

220. A data controller may delay or refuse (wholly or in part) to provide the data subject with information about data processing for law-enforcement purposes and the data subject's rights in relation to that processing if that is necessary to, among other things, (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences; (c) protect public security; or (d) protect national security (section 54(3) of the 2002 Act, transposing Article 13 § 3 of Directive (EU) 2016/680). When the obstacle ceases to exist, the data controller must provide the requested information within two months (section 54(4) of the 2002 Act).

221. The data subject's rights of access to, rectification, erasure and restriction of the processing of his or her personal data may be limited on the same grounds (sections 55(3) and 56(6) of the 2002 Act, transposing Articles 14, 15 §§ 1 and 2, and 16 § 4 of Directive (EU) 2016/680). When the obstacle ceases to exist, the data controller must provide the requested information within two months (sections 55(3) *in fine* and 56(6) *in fine* read in conjunction with section 54(4) of the 2002 Act). In any event, the controller must restrict the processing of personal data rather than altogether erase it if that data has to be maintained for the purposes of evidence (section 56(4)(2), transposing Article 16 § 3 (b) of the Directive).

222. If access to personal data is restricted under those provisions, the controller must inform the data subject of the restriction and the reasons for it within two months, but may omit doing so if that would defeat the purpose of the restriction (section 55(4) of the 2002 Act, transposing Article 15 § 3 of Directive (EU) 2016/680). In that case, the controller must document the factual or legal reasons on which that decision is based, and make those reasons available to the supervisory authorities (the Commission for Protection of Personal Data or the Inspectorate attached to the Supreme Judicial Council (section 55(5), transposing Article 15 § 4 of the Directive).

223. If rectification, erasure or restriction of the processing of personal data is refused under the above provisions, the controller must inform the data subject of the restriction and the reasons for it within two months, but may omit doing so if that would defeat the purpose of the refusal. In that case, the data controller must provide the reasons for the refusal to the data subject within two months after the obstacle ceases to exist (section 56(7) of the 2002 Act, transposing Article 16 § 4 of Directive (EU) 2016/680).

224. In all those cases of limitation on the rights of data subjects, they may exercise their rights indirectly, through the Commission for Protection of Personal Data or the Inspectorate attached to the Supreme Judicial Council (depending on whether the data are being processed by a judicial or a non-judicial authority – see paragraph 225 below). If they receive such a complaint, those authorities must check whether the limitation was lawful (section 57(1) of the 2002 Act, transposing Article 17 § 1 of Directive (EU) 2016/680). They must inform the data subject at least that all necessary checks have taken place, and of his or her right to seek a judicial remedy (section 57(2), transposing Article 17 § 3 of the Directive).

3. Supervisory authorities

225. The Commission for Protection of Personal Data supervises the processing of personal data for law-enforcement purposes by all authorities except the courts and the prosecuting and investigating authorities. The processing of personal data for law-enforcement purposes by the courts and the prosecuting and investigating authorities is supervised by the

Inspectorate attached to the Supreme Judicial Council (section 78 of the 2002 Act, transposing Article 41 of Directive (EU) 2016/680).

226. In carrying out that supervision, the Commission and the Inspectorate must, among other things, (a) examine complaints by data subjects, (b) check the lawfulness of the data processing in cases in which the data subject's rights have been restricted (see paragraphs 220 to 223 above), and (c) inform the data subject within three months of the outcome of the verification or of the reasons why one has not been carried out (section 79(1)(5) and (1)(6) of the 2002 Act, transposing Article 46 § 1 (f) and (g) of Directive (EU) 2016/680).

4. Remedies

227. Data subjects are entitled to the same remedies for alleged breaches of their rights by law-enforcement authorities as they are for alleged breaches of their rights by private persons (see paragraph 218 above) (section 82(1) of the 2002 Act, transposing Articles 52 § 1 and 54 of Directive (EU) 2016/680).

RELEVANT DECISIONS OF THE COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE

228. The Committee of Ministers of the Council of Europe has so far examined the execution of the Court's judgment in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) in March 2013, June 2017 and June 2019. The Committee is supervising that execution under its enhanced procedure, and the proceedings before it are still pending.

229. In its three decisions adopted so far in the course of that supervision (CM/Del/Dec(2013)1164/8; CM/Del/Dec(2017)1288/H46-7; and CM/Del/Dec(2019)1348/H46-5), the Committee noted the improvements resulting from the legislative reforms undertaken by the Bulgarian authorities in that domain, but also highlighted, *inter alia*, the following (outstanding) points of concern or uncertainty in relation to the general measures required to execute that judgment:

(a) the lack of clarity about whether surveillance could be used to protect national security if those to be placed under surveillance were not suspected of a criminal offence;

(b) the practical capacity of the courts receiving a high volume of surveillance applications – in particular the Specialised Criminal Court (see the table under paragraph 49 above) – to deal with those properly;

(c) the maximum duration of the initial authorisation of surveillance on national-security grounds (two years – see paragraph 79 (b) above);

(d) the lack of sufficient publicly available details about the procedures for screening and destroying information obtained through surveillance, and preserving its confidentiality and integrity (see paragraphs 87 to 99 above);

(e) the qualifications of the members of the National Bureau and their independence with respect to the authorities which they are tasked with overseeing (see paragraphs 109 and 112 *in fine* above); the possibility for the Bureau to access all materials which it needs to carry out its tasks, including the materials on which surveillance applications are based (see paragraphs 118 and 119 above); and the competence of the Bureau to notify legal persons – as opposed to individuals only – of unlawful surveillance (see paragraph 130 above); and

(f) the fact-finding capabilities of the civil courts in proceedings under section 2(1)(7) of the 1988 Act in situations in which the claimants have not been notified (or have learned otherwise) that they have been subjected to surveillance (see paragraphs 140 to 144 above), and the lack of certainty about the courts' powers to order the destruction of surveillance materials.

RELEVANT EUROPEAN UNION LAW

I. E-PRIVACY DIRECTIVE

230. By Article 15 § 1 of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ("E-Privacy Directive"), Member States may adopt legislative measures providing for the retention of communications data for a limited period, if that is justified by the need to "safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".

231. By Article 15 § 2 of the same Directive, read in conjunction with Article 94 § 2 of the GDPR, all provisions of the GDPR on judicial remedies relating to the processing of personal data apply with regard to national provisions adopted pursuant to the E-Privacy Directive.

II. DATA RETENTION DIRECTIVE

232. Article 3 read in conjunction with Article 5 and Article 6 of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks ("Data Retention Directive") required Member States to adopt measures to ensure that certain categories of communications data generated or processed by providers of (a) publicly available electronic communications services or of

(b) public communications networks within their jurisdiction were retained for periods ranging between six months and two years.

233. In a judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238) the CJEU held that Directive invalid as a whole, on the basis that it required a disproportionate interference with the rights to respect for private life and communications, protected under Article 7 of the Charter of Fundamental Rights of the European Union, and with the right to right to protection of personal data under Article 8 of the Charter. First, the Directive required the retention of all traffic data and applied to all means of electronic communication. Secondly, the Directive did not lay down substantive and procedural conditions governing access by the authorities to the retained data or to its subsequent use, and did not make such access dependent on a prior review by a court or by an independent administrative body whose decision could limit access to the data and its use to what was strictly necessary. Thirdly, the Directive required that all data be retained for a period of at least six months, without distinguishing between categories of data on the basis of its possible usefulness or the persons concerned. Lastly, the Directive did not set out sufficient safeguards for the effective protection of the retained data against the risk of abuse or against unlawful access and use.

III. GENERAL DATA PROTECTION REGULATION

234. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" – "GDPR") applies to "natural persons", and does not cover the processing of personal data which concerns legal persons (recital 14). By its Article 23 § 1, Member State legislation may restrict the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34 "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard", among other things, (a) national security, (b) public security, and (c) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

235. If relevant, any such legislation must, among other things, provide for the right of data subjects to be informed about the restriction, unless that may be prejudicial to its purpose (Article 23 § 2 (h) of the GDPR).

236. Each data subject is entitled to lodge a complaint with a supervisory authority if he or she "considers that the processing of personal data relating to him or her infringes [the GDPR]" (Article 77 § 1 of the GDPR).

237. Each data subject is also entitled, in the same circumstances, to an effective judicial remedy (Article 79 § 1 of the GDPR).

238. Any person who has suffered material or non-material damage as a result of an infringement of the GDPR is entitled to compensation from the controller or processor (Article 82 § 1 of the GDPR). Article 82 §§ 2 to 4 govern the modalities under which such compensation may be sought.

IV. LAW-ENFORCEMENT DIRECTIVE

239. Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data governs the processing of the personal data of "natural persons" by the competent authorities for the purposes of "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" (Articles 1 § 1 and 2 § 1). It had to be transposed by May 2018 (Article 63 § 1). Bulgaria did so, by way of an amendment to the 2002 Act, in March 2019 (see paragraphs 219 to 227 above).

V. CJEU CASE-LAW ON ARTICLE 15 § 1 OF THE E-PRIVACY DIRECTIVE

240. In a judgment of 21 December 2016 (*Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970), given pursuant to preliminary references by the Administrative Court of Appeal of Stockholm, Sweden, and the Court of Appeal of England and Wales, the CJEU held that national legislation providing for the general retention of all traffic and location data for the purpose of fighting crime was impermissible under Article 15 § 1 of the E-Privacy Directive (see paragraph 230 above). Article 15 § 1 also precluded legislation permitting the authorities to access retained data if, so far as relevant for the purposes of the present case, (a) the objective was not restricted to fighting serious crime, and (b) such access was not subject to prior review by a court or an independent authority. The CJEU based those conclusions on, among other things, the E-Privacy Directive's overall structure, including the general principle of confidentiality of communications laid down by it, and the requirement of strict necessity under European Union law for any limitations on the protection of personal data. Lastly, the CJEU declined to answer a question about whether the protection conferred by Articles 7 and 8 of the Charter, as construed by it, was wider than that under Article 8 of the Convention. It noted, among other things, that European Union law could give more

extensive protection than the Convention, and that Article 8 of the Charter concerned a right (the protection of personal data) which had no equivalent in the Convention.

241. In a judgment of 2 October 2018 (*Ministerio Fiscal*, C-207/16, EU:C:2018:788), given pursuant to a preliminary reference by the Provincial Court of Tarragona, Spain, the CJEU held that the interference entailed by access to retained names and addresses to identify the owners of SIM cards activated with a stolen mobile telephone was not sufficiently serious, and was thus permissible under Article 15 § 1 of the E-Privacy Directive even if not justified by the need to fight "serious" crime.

242. In a judgment of 6 October 2020 (*La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791), given pursuant to preliminary references by the French Council of State and the Belgian Constitutional Court, the CJEU, among other things, confirmed its position in *Tele2 Sverige and Watson and Others* (see paragraph 240 above) that Article 15 § 1 of the E-Privacy Directive precluded the general retention of traffic and location data for the purpose of fighting serious crime, and held that this provision permitted solely a targeted retention of such data, limited on the basis of objective and non-discriminatory factors. By contrast, Article 15 § 1 did not preclude the general retention of (a) IP addresses assigned to the source of an Internet connection, and (b) data relating to the civil identity of users of communications systems. General retention of traffic and location data – for a (renewable) period limited to what was strictly necessary – was, however, permissible if a State was facing a genuine and serious national-security threat which was present or foreseeable. But the decision citing such a threat to require general retention had to be subject to effective review, either by a court or by an independent administrative body whose decision was binding. That review had to extend also to whether the conditions and safeguards which had to be laid down were observed.

243. In another judgment of 6 October 2020 (*Privacy International*, C-623/17, EU:C:2020:790), given pursuant to a preliminary reference by the United Kingdom's Investigatory Powers Tribunal, the CJEU held, among other things, that Article 15 § 1 of the E-Privacy Directive precluded legislation enabling an authority to require communications service providers to carry out a general transmission of traffic and location data to the security and intelligence agencies for the purpose of safeguarding national security.

244. In a judgment of 2 March 2021 (*Prokuratuur*, C-746/18, EU:C:2021:152), given pursuant to a preliminary reference by the Supreme Court of Estonia, the CJEU reiterated that Article 15 § 1 of the E-Privacy Directive permitted access to retained traffic or location data for the purpose of fighting crime only when it came to serious crime or serious threats to public security, regardless of the length of the period in respect of which

access was sought and the quantity or nature of the data available in respect of that period. The CJEU went on to hold that the power to examine access requests could not be given to a prosecutor's office, since its tasks of directing pretrial proceedings and prosecuting affected its independence *vis-à-vis* the parties to the criminal proceedings.

245. Three preliminary references concerning the compatibility of the German and Irish laws requiring the general retention of communications data with Article 15 § 1 of the E-Privacy Directive, made respectively by the German Federal Administrative Court in October 2019 and by the Supreme Court of Ireland in March 2020 (*SpaceNet*, C-793/19; *Telekom Deutschland*, C-794/19; and *Commissioner of the Garda Síochána and Others*, no. C-140/20) are still pending.

THE LAW

I. SECRET SURVEILLANCE

246. The applicants complained that the system of secret surveillance in Bulgaria did not meet the requirements of Article 8 of the Convention, and that they did not have effective remedies in that respect, in breach of Article 13 of the Convention.

247. In the light of the Court's case-law (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 307, ECHR 2015), the complaint falls to be examined solely under Article 8 of the Convention, which provides, so far as relevant:

> "1. Everyone has the right to respect for his private ... 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

1. The parties' submissions

(a) Victim status of the applicants

(i) The Government

248. The Government submitted that the applicants could not claim to be victims of a violation of their right to respect for their private life or correspondence. That was because under Bulgarian law only people suspected of serious criminal offences could be placed under surveillance, even when national security was at stake. Nothing suggested that any of

applicants fell into that category, and that possibility was altogether inconceivable for the two applicant organisations, since in Bulgaria legal persons could not bear criminal liability.

249. Moreover, none of the applicants, who had the requisite expertise, had asked the National Bureau whether special means of surveillance had been used with respect to them. Nor had the two individual applicants tried to bring a claim under section 2(1)(7) of the 1988 Act, which could be brought even without a notification by the Bureau that special means of surveillance had been used against them. Both of those were effective remedies. It followed that the applicants had to show that they were at risk of surveillance owing to their personal situation – something which they had not done, and which was hard to believe, since nothing suggested that they could be suspected of any of the criminal offences justifying surveillance in Bulgaria.

(ii) The applicants

250. The applicants replied that under the system of secret surveillance in Bulgaria the communications of anyone in the country could be intercepted, for several reasons. First, the laws permitting surveillance were couched in broad and vague terms, especially as regards the notion of national security. Secondly, many authorities could request surveillance, and the prosecuting authorities could uncontrollably open criminal proceedings against anyone. Thirdly, authorisation procedures were routinely flouted. Lastly, oversight by the National Bureau was ineffective in practice, which had made it pointless for the applicants to complain to it, especially since they could be subjected to surveillance indirectly, through the placing of contacts of theirs under surveillance. They had not brought a claim under section 2(1)(7) of the 1988 Act since it would have been ineffective in their situation, and was moreover not available to the two applicant organisations, since it was open only to individuals. It was thus unnecessary for any of them to show that they were at risk of being subjected to surveillance owing to their personal situation.

(b) Exhaustion of domestic remedies

251. Based on the considerations summarised in paragraph 249 above, the Government further argued that the applicants had not exhausted domestic remedies.

252. The applicants replied that, for the reasons summarised in paragraph 250 above, the remedies suggested by the Government were not effective in their situation.

2. The Court's assessment

(a) Whether the complaint is "substantially the same"

253. The first question which arises is whether the present complaint is "substantially the same" as that examined in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (no. 62540/00, 28 June 2007). The Court must deal with the point on its own initiative, since it marks out the limits of its competence (see *Harkins v. the United Kingdom* (dec.) [GC], no. 71537/14, § 55, 15 June 2017).

254. The Court finds this not to be so, for the following reasons.

255. It is true that two of the applicants – Mr Ekimdzhiev and the Association for European Integration and Human Rights – are the same as in that earlier case, and that the gist of their grievance here, as formulated by them, is identical to the gist of the grievance examined there. The present complaint is, however, not based on the same facts. In that earlier case, the Court scrutinised the system of secret surveillance in Bulgaria as it stood in mid-2007, whereas in the case at hand it must scrutinise that system as it stands now (see paragraph 293 below). The relevant statutory and regulatory provisions in Bulgaria have evolved considerably since 2007, as has the manner of their application (see in particular paragraphs 13 to 16 above). All that is "relevant new information" within the meaning of Article 35 § 2 (b) of the Convention (see, *mutatis mutandis*, *Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland (no. 2)* [GC], no. 32772/02, §§ 64-65, ECHR 2009, and *Ivanţoc and Others v. Moldova and Russia*, no. 23687/05, § 93, 15 November 2011). Admittedly, that expression must be construed to mean relevant new *factual* information (see *Harkins*, cited above, § 50). But in cases such as the one at hand, where the complaint is based on the state of the domestic law rather than on its application in a specific instance, that domestic law and the way it is applied in general is the main fact under examination.

(b) Whether the Court is prevented from examining the complaint by Article 46 of the Convention

256. The second question which arises is whether the Court is prevented from examining the complaint by Article 46 of the Convention. That point, which goes to the Court's jurisdiction, must likewise be examined on its own initiative. It is closely linked with the issue examined in paragraphs 253 to 255 above.

257. The Committee of Ministers' ongoing review of the Bulgarian laws and practices relating to secret surveillance in the exercise of its task of supervising the execution of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraphs 228 and 229 above) is no bar to the admissibility of the complaint. The Court's task in this case is not to assess whether the general measures taken by the

Bulgarian authorities were sufficient to discharge their duty under Article 46 § 1 of the Convention to abide by that judgment; the Court has no jurisdiction to do so (see *Ivanţoc and Others*, cited above, § 91). Its task here is rather to examine whether the complaint that the system of secret surveillance in Bulgaria, as it stands now – granted, partly as a result of general measures taken to abide by *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 14 above) – falls short of the requirements of Article 8 of the Convention is admissible and well-founded. Although that examination may in practice overlap or even in parts coincide with the supervision carried out by the Committee of Ministers, that does not take the complaint outside the Court's jurisdiction. The Committee of Ministers' role in the execution of the Court's judgments does not mean that measures taken by a respondent State to remedy a violation found by the Court cannot raise a new issue undecided by the earlier judgment and, as such, form the subject of a new application with which the Court may deal (see *Verein gegen Tierfabriken Schweiz (VgT) (no. 2)*, cited above, § 62; *Bochan v. Ukraine (no. 2)* [GC], no. 22251/08, § 33, ECHR 2015; and *Moreira Ferreira v. Portugal (no. 2)* [GC], no. 19867/12, § 47 (b), 11 July 2017). In this context, "new issue" connotes the existence of "relevant new information" within the meaning of Article 35 § 2 (b) of the Convention (see *Verein gegen Tierfabriken Schweiz (VgT) (no. 2)*, § 63; *Ivanţoc and Others*, § 85; and *Moreira Ferreira*, § 47 (d), all cited above). But, as noted in paragraph 255 above, such "relevant new information" is present in this case (compare, *mutatis mutandis*, with *Mehemi v. France (no. 2)*, no. 53470/99, §§ 43-44, ECHR 2003-IV; *Wasserman v. Russia (no. 2)*, no. 21071/05, §§ 34-37, 10 April 2008; *Liu v. Russia (no. 2)*, no. 29157/09, §§ 62-67, 26 July 2011; *Ivanţoc and Others*, cited above, §§ 89-95; and *V.D. v. Croatia (no. 2)*, no. 19421/15, §§ 49-54, 15 November 2018).

258. The Court therefore has jurisdiction to examine the complaint.

(c) The applicants' victim status and exhaustion of domestic remedies

259. The Government's objections that the applicants cannot claim to be victims of a violation and that they have not exhausted domestic remedies are both so closely linked to the substance of the applicants' complaint that they must be joined to its merits (see *Roman Zakharov*, cited above, § 150).

(d) Conclusion about the admissibility of the complaint

260. The complaint is, moreover, not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention or inadmissible on other grounds. It must therefore be declared admissible.

B. Merits

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

(a) The parties' submissions

261. The parties' submissions on these points are summarised in paragraphs 248 to 250 above.

(b) The Court's assessment

(i) General principles

262. The general principles on when applicants may claim that they are victims of an interference with their rights under Article 8 of the Convention owing to the mere existence of domestic laws or practices permitting secret surveillance were clarified in *Roman Zakharov* (cited above, § 171) and more recently reiterated in *Centrum för rättvisa v. Sweden* ([GC], no. 35252/08, § 167, 25 May 2021).

(ii) Application of those principles

(α) Scope of the relevant law

263. Under the terms of section 12 of the 1997 Act, special means of surveillance can be used with respect to, *inter alia*, (a) persons suspected of, or unwittingly used for, the preparation or commission of one or more of the serious offences listed in section 3(1) of the 1997 Act; (b) persons or objects related to national security; and (c) objects necessary to identify such persons (see paragraph 23 above). The wording of section 12 thus suggests that national security can be a standalone ground for resorting to secret surveillance; this also follows from section 4 (see paragraph 22 above). But even if it is accepted that, as asserted by the Government with reference to the wording of section 14 of the 1997 Act (see paragraph 22 above), under Bulgarian law national security cannot be a standalone ground for resorting to secret surveillance, it remains the case that theoretically any individual in the country can be suspected of being involved, wittingly or unwittingly, in the planning or commission of a relevant criminal offence, and thus be him- or herself subjected to surveillance. It is also readily apparent that, regardless of whether they have themselves been placed under surveillance, individuals – or legal persons – can have their communications intercepted indirectly, as a result of the surveillance of another individual falling in one of the categories laid down in section 12 of the 1997 Act. It follows that all four applicants, including the two applicant organisations, may possibly be affected by the contested legislation. It is true that some surveillance techniques, such as visual surveillance and tracking (see paragraph 11 above), cannot be applied to legal persons as such. But it appears that in many cases the surveillance warrants authorise the use of those techniques

alongside other surveillance techniques, such as tapping, which can affect the communications of legal persons (see paragraphs 61 and 65 above).

(β) Availability of an effective remedy

264. The next question is whether there exists in Bulgaria an effective remedy which can alleviate the suspicion among the general public that secret surveillance powers are being abused.

265. In 2009 Bulgaria put in place a dedicated remedy in respect of secret surveillance, in the form of a claim for damages under section 2(1)(7) of the 1988 Act (see paragraph 136 above). The Court has recognised that such a claim is an effective remedy for people who have already learned that they have been subjected to surveillance as a result of criminal proceedings, in cases when the surveillance has taken place after the entry into force of that provision (see *Harizanov v. Bulgaria* (dec.), no. 53626/14, §§ 94-99, 5 December 2017).

266. But that only concerns situations in which the surveillance has yielded information which has led to the production of evidentiary material later used – and hence disclosed – in criminal proceedings. Throughout the past decade, the instances of surveillance which have led to the production of such evidentiary material have ranged from about 24% to about 60% (see the table under paragraph 93 above). And it is far from certain that in all of those cases such evidentiary material has later led to the bringing of charges, and has thus been disclosed to the persons concerned in the context of criminal proceedings.

267. It appears that in all cases in which that has not happened, the only (lawful) way in which the people concerned can learn that they have been subjected to surveillance is a notification by the National Bureau. But the 1997 Act does not require that all such people be notified. Irrespective of whether it investigates on its own initiative or pursuant to a complaint by someone suspecting that he or she has been subjected to surveillance, the Bureau is only required to notify people subjected to surveillance unlawfully (as determined by it), and even then only if that notification would not defeat the purpose of the surveillance or reveal the technical or operational means whereby it has been carried out (see paragraph 130 above). In practice, the Bureau notifies few people, if any, each year, even in comparison to the number of complaints it receives (see the table under paragraph 135 above). It appears that in other cases it simply informs the people who have applied to it that they have not been subjected to unlawful surveillance, without specifying whether that means that (a) no surveillance has taken place, that (b) it has taken place but was lawful, or (c) that it was indeed unlawful but should not be revealed because doing so would defeat its purpose or reveal the technical or operational means whereby it has been carried out (see paragraph 131 above). In hypothesis (c), the wording of the Bureau's notification, as transpiring from the three examples made available

to the Court (see paragraph 131 above), would in fact be misleading since there has been unlawful surveillance but there are grounds to conceal that it has taken place. The recipients of such notifications have no means of challenging them and thus obtaining more information (see paragraph 133 above).

268. Moreover, contrary to what was asserted by the Government, it does not seem that proceedings for damages under section 2(1)(7) of the 1988 Act (see paragraph 136 above) are, as matters stand, available to people who have not been notified by the National Bureau that they have been subjected to surveillance or have learned about that surveillance as a result of criminal proceedings in which its results have been used. It is true that section 2(1)(7) does not by its terms elevate such notification into a condition for the admissibility of such claims. But although that provision has already been in effect for more than twelve years, no cases have been reported in which claims under it have been successfully brought blindly, in the absence of prior notification by the Bureau or of information about surveillance which has emerged in criminal proceedings (see paragraph 140 above). Indeed, the apparently limited fact-finding capabilities of the civil courts in proceedings under section 2(1)(7) have already been noted by the Committee of Ministers in the context of its supervision of the execution of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 229 (f) above).

269. The manner in which the Bulgarian courts have applied the rules of evidence in such cases suggests that absence of a notification by the National Bureau or of information about surveillance which has emerged in criminal proceedings is likely to be an unsurmountable obstacle to pursuing such claims (see paragraphs 141, 142 and 144 above). That was recognised, even if indirectly, by the Supreme Court of Cassation, which held that the limitation period for bringing such a claim starts to run when the person concerned is notified by the Bureau, because without such notification that person has no means of vindicating his or her rights (see paragraph 138 (h) above). In a recent case, the Burgas Regional Court even expressly held that a claim under section 2(1)(7) of the 1988 Act could be brought only if the use of special means of surveillance with respect to the claimant was apparent either from the materials adduced as evidence in a criminal case or from a notification by the Bureau (see paragraph 143 above).

270. In the absence of reported decisions by the Bulgarian courts, it is not for this Court to say whether or how the rules of civil procedure in Bulgaria which govern the disclosure of documents by the opposing party, by a third party or by a public authority (see paragraphs 146 to 150 above) can be applied in such cases. It was for the Government to explain that point, and as far as possible support their explanations with concrete examples (see, *mutatis mutandis*, *Roman Zakharov*, cited above, § 295, and *Mustafa Sezgin Tanrıkulu v. Turkey*, no. 27473/06, §§ 28-29, 18 July 2017).

It suffices to note that for twelve years there have apparently been no cases in which those procedural tools have been deployed to overcome the absence of a prior notification by the National Bureau or of information about surveillance which has emerged in criminal proceedings.

271. Another obstacle for those wishing to bring such a claim blindly is identifying the correct defendant, which must be done at the outset of the proceedings (see paragraph 138 (c) above), but may nevertheless be impossible in the absence of any information about which authority has requested the surveillance or has carried it out (see, *mutatis mutandis*, *Ribcheva and Others v. Bulgaria*, nos. 37801/16 and 2 others, § 149 *in fine*, 30 March 2021).

272. A further limitation of the remedy under section 2(1)(7) of the 1988 Act lies in the degree of scrutiny applied by the courts when hearing such claims. The Supreme Court of Cassation has held that when deciding such claims the courts cannot inquire whether the judges who have issued a surveillance warrant have correctly assessed the need to do so (see paragraph 138 (f) above). That means the courts may check for formal deficiencies but cannot delve into the most important issues – whether the surveillance whose lawfulness is being challenged before them was based on a reasonable suspicion and amounted to a proportionate interference with the claimant's rights under Article 8 of the Convention. This limitation deprives this safeguard from much of its efficacy.

273. Lastly, as is apparent from the provision's wording (see paragraph 136 above), such claims are not open to legal persons.

274. Owing to all of these limitations, the remedy provided by section 2(1)(7) of the 1988 Act cannot sufficiently dispel the public's misgivings about the threat of abusive secret surveillance.

275. Nor can those misgivings be dispelled by other possible remedies. The Government did not argue, and there is no indication, that there have so far been any instances in which someone has been able to obtain the destruction of data obtained through surveillance in reliance on section 56(6) *in fine* of the 2002 Act, amended in 2019 to transpose Directive (EU) 2016/680 (see paragraph 221 above), to obtain redress by way of a complaint to the Commission for Protection of Personal Data or the Inspectorate attached to the Supreme Judicial Council under section 57 of that Act (see paragraph 224 above), or to obtain redress by way of a judicial remedy under section 82(1) of the 2002 Act, both likewise added in 2019 (see paragraph 227 above). It is true that those provisions are novel, and that they are part of a branch of law which has only developed relatively recently. But in the absence of any information about the way in which they can operate with respect to data obtained by way of secret surveillance (contrast the circumstances in *Tretter and Others v. Austria* (dec.) [Committee], no. 3599/10, §§ 10-14 and 43-46, 29 September 2020), it is

not for the Court to speculate on the point. Those remedies are, moreover, not available to legal persons (see paragraphs 216 and 239 above).

(γ) Conclusion

276. In view of the above considerations, there is no need to check whether the applicants are at risk of having their communications intercepted owing to their personal situation (see, *mutatis mutandis*, *Centrum för rättvisa*, cited above, §§ 175-76).

277. It follows that an examination of the relevant laws and practices in the abstract is justified. It also follows that the Government's objection that the applicants may not claim to be victims of a violation of Article 8 of the Convention allegedly caused by the mere existence of laws permitting secret surveillance, which was joined to the merits (see paragraph 259 above), must be rejected.

2. Justification for the interference

(a) The parties' submissions

(i) The applicants

278. The applicants submitted that the legislation governing secret surveillance, as applied in practice by the authorities, did not provide enough guarantees against the abusive surveillance of anyone in Bulgaria.

279. In their view, the notion of national security, as understood in Bulgaria, was too vague, and permitted even legitimate political activities by the opposition to be seen as sufficient grounds for surveillance. The maximum possible length of the initial authorisation in such cases – two years – rendered all other safeguards nugatory. The clause authorising surveillance without prior judicial authorisation in urgent cases was also particularly prone to abuse. The number of authorities which could request surveillance outside the framework of already pending criminal proceedings had increased throughout the years. For their part, the prosecuting authorities could obtain abusive and arbitrary surveillance in criminal proceedings by opening them without proper justification, which could not be controlled by the courts at the pre-trial stage or engage the personal liability of the public prosecutors doing so. The genuineness of the risk of such abuses had been illustrated by the publication in February 2020, on the initiative of the Chief Prosecutor, of intercepted conversations between the President of the Republic, who enjoyed full immunity from prosecution, and the commander of the Air Force.

280. Many of the safeguards surrounding the authorisation procedure were in practice not adhered to, as recorded in several reports and publications. The courts often issued surveillance warrants without properly checking whether it was justified to do so – a practice which had reached its highpoint in the warrant in relation to which the 2011-15 President of the

Sofia City Court had been criminally convicted. Judicial oversight of the storage and destruction of surveillance materials was also ineffective.

281. Oversight by the National Bureau was likewise ineffective. Most of the Bureau's current members had come from the security services and did not have proper legal qualifications. Owing to the requirement to undergo security vetting by the State Agency for National Security and keep their security clearance throughout their term of office, Bureau members could lose their posts as a result of steps taken by that Agency, which was one of the authorities which most often requested surveillance. That risk was not merely theoretical, as illustrated by the case of the Bureau's first deputy chairperson. This had seriously affected the Bureau's independence and had marginalised it, especially in the last few years. Several interviews and declarations of the Bureau's first chairperson had highlighted the weakening of its role and of its supervision over the prosecuting authorities and the State Agency for National Security. Another issue had been the illegal curtailing of the possibility for the Bureau to access materials held by the prosecuting authorities. Lastly, the Bureau checked solely the surveillance's formal legality, and only notified those concerned if they had been subjected to it unlawfully. That explained the small number of notifications made by the Bureau, which was insignificant if compared to the number of surveillance operations.

282. The dedicated remedy, a claim under section 2(1)(7) of the 1988 Act, was not available to legal persons, and, as illustrated by the courts' case-law, only worked when the Bureau had notified those concerned of unlawful surveillance. In such proceedings, the courts could not obtain the primary materials and had to rely on information provided by the Bureau.

(ii) The Government

283. The Government pointed out that most rules governing the use of special means of surveillance were contained in legislative enactments. Those enactments and all relevant regulations had been published. There were also internal rules on the procedures for storing and destroying materials obtained via surveillance and the resulting evidence. The National Bureau supervised whether those rules were in line with the relevant statutes and regulations.

284. The law furthermore laid down an exhaustive list of offences which could trigger surveillance. Although it also provided that it could be employed to protect national security, in the courts' practice that was not a standalone ground to authorise surveillance; even when national security was at stake, this could be done only to prevent or investigate one of the offences listed in the law, which was a safeguard against abusive interpretations of the notion of national security. The law also specified the categories of persons who could be subjected to surveillance, as well as the

grounds and conditions on which, and the purposes for which, surveillance could be authorised and carried out.

285. Surveillance was subject to prior judicial authorisation except in urgent cases – an exception to which the authorities resorted sparingly. Even in those cases, surveillance had to be validated retrospectively by a judge within twenty-four hours, and that judge could also assess whether it had been justified to resort to the urgent procedure. To obtain a warrant, the relevant authority had to make a reasoned application, and when examining that application the judge could request all supporting materials. The decision to issue a surveillance warrant had to be reasoned, and the judge reviewed whether all legal requirements were in place – including whether it was justified to resort to surveillance – on the basis of all materials in the case file rather than simply those provided by the requesting authority. That was a strong safeguard against frivolous or unfounded surveillance applications based on trumped-up charges. By law, the judge had up to forty-eight hours to consider the application, which was enough to permit proper review. That was important for courts receiving many surveillance applications.

286. The law set out clearly the maximum duration for which surveillance could be authorised. Although the maximum statutory periods for surveillance on national-security grounds were long – initially up to two years and altogether up to three years – in practice the courts never issued surveillance warrants for periods exceeding six months.

287. The judges who had authorised the surveillance could then oversee the way in which it had been carried out, since the requesting authority had to report to them and provide all surveillance results and any evidence produced on their basis. Judges could also seek additional materials. That form of ongoing supervision supplemented that by the National Bureau.

288. The statutory rules governing the screening, processing, storage and destruction of surveillance materials were sufficiently precise, and were supplemented by internal rules which were subject to supervision by the National Bureau. The general position was that any materials not used for evidence were to be destroyed quickly, the only exception being those relating to offences against national security, which were to be kept for fifteen years. Although the various rules, which differed depending on whether the materials contained classified information, had not been codified in a single enactment, they were all clear enough and contained sufficient safeguards against abuse.

289. As regards the National Bureau, its members were elected by and only accountable to Parliament. They had to meet stringent requirements and have high professional qualifications. Even if some of those members had no legal education or experience, that did not mean that they were not suitably qualified. It was true that upon nomination all members had to undergo security vetting by the State Agency for National Security, but that

was inevitable when it came to sensitive information, and any revocation of their security clearance was amenable to judicial review. The Bureau had extensive inspection powers and could give instructions to the relevant authorities, which it did regularly, including with respect to the State Agency for National Security. No incidents casting doubt on the independence or integrity of any Bureau members had been brought to the attention of Parliament. Additional supervision of the system was ensured by the parliamentary committee.

290. Lastly, both the notification procedure and its limitations were fully consistent with the requirements of the Court's case-law. Legal persons could obtain such notification as well, as illustrated by a case relating to a mobile telephone line subscribed by a bank in which the National Bureau had investigated a complaint about alleged tapping of that line by the bank's management. The dedicated remedy – a claim under section 2(1)(7) of the 1988 Act – worked well when there had been notification by the Bureau, but could operate properly also in the absence of such notification, although there had so far been no such cases. Notification was not a formal prerequisite for bringing such a claim, and anyone could bring one simply on the basis of a suspicion of having been subjected to surveillance. If the claimant was unable to adduce evidence of that, the court dealing with the case could request such evidence from the relevant authorities or order the Bureau to investigate the case and report back. Legal persons could also use that remedy and obtain an award of damages.

(b) The Court's assessment

(i) General principles

291. The general principles governing the question when secret measures of surveillance, including the interception of communications, can be justified under Article 8 § 2 of the Convention were set out in detail in *Roman Zakharov* (cited above, §§ 227-34, 236, 243, 247, 250, 257-58, 275, 278 and 287-88). Many of those principles were recently reiterated, although in relation to a somewhat different context – bulk interception – in *Centrum för rättvisa* (cited above, §§ 246-53) and *Big Brother Watch and Others v. the United Kingdom* ([GC], nos. 58170/13 and 2 others, §§ 332-39, 25 May 2021).

292. It is not necessary to repeat all of them here, except to emphasise that the overarching requirement is that a secret surveillance system must contain effective guarantees – especially review and oversight arrangements – which protect against the inherent risk of abuse and which keep the interference which such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society".

293. In cases such as the present one, in which the applicants complain in the abstract about a system of secret surveillance rather than of specific instances of such surveillance, the relevant national laws and practices are to be scrutinised as they stand when the Court examines the admissibility of the application rather than as they stood when it was lodged (see *Centrum för rättvisa*, § 151, and *Big Brother Watch and Others*, § 270, both cited above). The other point of particular relevance to this case is that the assessment of whether the laws at issue offer effective guarantees must be based not only the laws as they exist in the statute book, but also on (a) the actual operation of the surveillance regime, and (b) the existence or absence of evidence of actual abuse (see *Centrum för rättvisa*, § 274, and *Big Brother Watch and Others*, § 360, both cited above).

(ii) Application of those principles

294. In *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, §§ 79-84) the Court examined the system of secret surveillance in Bulgaria, as in force in mid-2007. It found that the procedure for authorising surveillance, if strictly adhered to, offered sufficient protection against arbitrary or indiscriminate surveillance. It went on to find deficiencies in relation to the following points: (a) lack of review by an independent body of the implementation of surveillance measures or of whether the material obtained through such measures would be destroyed within the time-limits if the surveillance had proved fruitless; (b) lack of sufficient safeguards in respect of surveillance on national security grounds and outside the context of criminal proceedings; (c) lack of regulations specifying with an appropriate degree of precision the manner of screening of surveillance materials, or the procedures for preserving their integrity and confidentiality and the procedures for their destruction; (d) lack of an independent body overseeing the functioning of the system of secret surveillance; (e) lack of independent control over the use of materials falling outside the scope of the original surveillance application; and (f) lack of notification of the persons concerned under any circumstances (ibid., §§ 85-91). On that basis, the Court concluded that Bulgarian law did not provide sufficient guarantees against the risk of abuse inherent in any system of secret surveillance (ibid., § 93).

295. Since that judgment, and partly it seems as a result of it, Bulgarian law governing secret surveillance had evolved considerably. All the same, the Committee of Ministers has not yet adopted a final resolution concluding that its functions relating to the supervision of the execution of that judgment have been completed; it has identified several outstanding points of concern in relation to the general measures taken by the Bulgarian authorities to implement that judgment (see paragraphs 228 and 229 above). For its part, the Court must, as already noted, examine not whether the Bulgarian authorities have executed that judgment, but whether the relevant

Bulgarian law, as it stands now, meets the requirements of Article 8 of the Convention (see paragraph 257 above).

(α) Accessibility of the law

296. All statutory provisions governing secret surveillance in Bulgaria, as well as the internal rules of the National Bureau for Control of Special Means of Surveillance (see paragraph 13 above), have been officially published and are thus accessible to the public. By contrast, the internal storage and destruction rules mentioned by the Government (see paragraphs 283 and 288 above) have apparently not been made accessible to the public.

297. For its part, the Chief Prosecutor's instruction governing the deliberate or accidental use of special means of surveillance with respect to lawyers, although not published by the authorities, was published in the Supreme Bar Council's journal (see paragraphs 27 to 30 above). It can be accepted that this made it sufficiently accessible for the persons that it concerns – practising lawyers such as the first and third applicants and organisations specialising in legal issues such as the second and fourth applicants (see, *mutatis mutandis*, *Groppera Radio AG and Others v. Switzerland*, 28 March 1990, § 68, Series A no. 173, and *Autronic AG v. Switzerland*, 22 May 1990, § 57, Series A no. 178).

(β) Grounds on which secret surveillance may be resorted to and persons who can be placed under surveillance

298. The relevant issue in relation to the grounds on which secret surveillance may be resorted to and the persons who can be placed under surveillance is whether the law authorising or permitting surveillance lays down with sufficient clarity (a) the nature of the offences and other grounds which may give rise to surveillance and (b) the categories of persons who may be placed under surveillance.

299. In Bulgaria, the law sets outs in an exhaustive manner the serious intentional criminal offences which can trigger the use of special means of surveillance (see paragraph 18 above). Moreover, it specifies that such means can be used only if there are grounds to suspect that such an offence is being planned, or is being or has been committed, and only if other methods of detection or investigation would be unlikely to succeed (see paragraphs 18 and 20 above). The law is thus sufficiently clear on that point (see *Roman Zakharov*, cited above, § 244). Indeed, it is clearer than when the Court first examined it and found it adequate in this respect in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, §§ 10 and 79). Although the types of offences falling into that list are varied, it appears that in practice in the vast majority of cases the authorities resort to surveillance in relation to the offences of (a) being the

leader or member of a criminal gang and of (b) dealing in narcotic drugs (see the table under paragraph 19 above).

300. It is true that the law says that special means of surveillance can also be used for "activities relating to national security" (see paragraph 22 above). In the absence of more detailed information about the practice of the relevant Bulgarian courts and authorities on that point, it is difficult to check whether, as asserted by the Government (see paragraph 22 above), national security can never be a standalone ground for surveillance in Bulgaria. The statutory requirement that each surveillance application contain a full account of the circumstances which give cause to suspect that a relevant offence is being prepared or committed or has been committed, including when it comes to national security (see paragraph 39 above), and the wording of the provision which lays down the time-limit for using special means of surveillance to protect national security, which appears to link that with the prevention of offences against the Republic (see paragraph 79 (b) above) appear to support the Government's submission. It remains unclear, however, how those provisions are being applied in practice. The lack of clarity on this point was already noted by the Committee of Ministers in the context of its supervision of the execution of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 229 (a) above).

301. But even if it is accepted that under Bulgarian law the protection of national security can be a standalone ground for secret surveillance, that does not in itself contravene Article 8 of the Convention (see *Association for European Integration and Human Rights and Ekimdzhiev*, § 84; *Centrum för rättvisa*, § 261; and *Big Brother Watch and Others*, § 347, all cited above). What rather matters is that any potential abuses flowing from the inherently vague meaning and contours of the notion of national security can be checked. It must be noted in this connection that even when it comes to national security, the relevant authorities must seek judicial authorisation for the surveillance, which can limit their discretion in interpreting that notion and ensure that sufficient reasons to place someone under surveillance are present in each case (see *Roman Zakharov*, cited above, § 249). This is an important safeguard against arbitrariness and abuse. Its effectiveness is analysed in paragraphs 307 to 322 below.

302. The law also sets out in an exhaustive manner the categories of persons who, or objects which, may be placed under surveillance. When it comes to surveillance relating to criminal offences, the relevant categories are clearly defined: those are either people suspected of committing offences, people unwittingly used for their preparation or commission, people who have agreed to surveillance for their own protection, or cooperating witnesses in cases relating to a limited class of serious intentional offences, as well as objects capable of leading to the identification of such persons if their identity is unknown (see

paragraph 23 (a), (c), (d) and (e) above). It is true that when it comes to surveillance on national-security grounds, the law is couched in vaguer terms: "persons or objects related to national security" (see paragraph 23 (b) above). But the considerations in paragraph 301 above about the possibility of checking potential abuses flowing from the vagueness of the notion of national security are equally relevant here.

303. A problem arises, however, with the lack of sufficient precision about the meaning of the term "objects" in section 12(1) of the 1997 Act (see paragraph 23 (b) and (c) above). The Act does not clarify whether the "objects" which may be placed under surveillance – either because they relate to national security or because they are necessary to identify persons who need to be placed under surveillance – need to be concrete (for instance, specific premises, a specific vehicle, or a specific telephone line). It must be noted in this connection that the secret surveillance regime in Bulgaria is intended to be a targeted regime rather than a bulk one (compare with *Roman Zakharov*, cited above, § 265). Although an extreme example, the case of *Mustafa Sezgin Tanrıkulu* (cited above, §§ 51-60) illustrates the risk of misinterpretation of insufficiently precise legal provisions normally meant to permit only targeted surveillance to in reality enable large-scale surveillance. So do the facts underlying the 2016 criminal conviction of the President of the Sofia City Court (see paragraph 56 above). In 2014 she had authorised the surveillance of an automated police information system (which itself surely contained data about many persons), apparently considering that that system was an "object" within the meaning of section 12(1) of the 1997 Act. She was then charged with authorising surveillance with respect to an "object" which did not properly fall within the statutory definition, but the courts acquitted her of that charge and found her guilty solely with respect to the time-limit of the authorisation which she had issued. Although as a result of the non-publication of the relevant judgments the reasons underlying that acquittal remain unclear, it tends to suggest than the Bulgarian courts are not averse to construing the term "objects" in section 12(1) of the 1997 Act in a rather extensive way.

304. In the light of these considerations, it can be said that Bulgarian law complies with the requirements of Article 8 of the Convention in respect of the grounds on which secret surveillance may be resorted to and persons who can be placed under surveillance, except for the lack of a more precise definition of the term "objects" in section 12(1) of the 1997 Act (see paragraph 23 (b) and (c) above).

(γ) Duration of secret surveillance measures

305. Bulgarian law lays down clearly the initial and maximum duration of secret surveillance measures (see paragraph 79 above). It is also clear that surveillance beyond the initially authorised period is only possible if authorised by the competent judge, who must be presented not only with the

same information as that required for the initial authorisation, but also with a full account of any surveillance results obtained so far (see paragraph 42 above). Lastly, the law sets out the circumstances in which surveillance must be stopped (see paragraph 82 above). There is, all the same, one area of concern, and that is the potential duration of the initial authorisation for surveillance on national-security grounds, which is up to two years (see paragraph 79 (b) above). The sheer length of that period, coupled with the inherently unclear contours of the notion of national security, significantly weakens the judicial control to which such surveillance must be subjected. This point has already been noted by the Committee of Ministers in the context of its supervision of the execution of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 229 (c) above). Even if, as asserted by the Government (see paragraph 286 above), in practice the courts never issue such warrants for periods exceeding six months, that is not based on any statutory limitation.

(δ) Authorisation procedures

306. The relevant factors under this rubric are (a) the status of the authority which can authorise secret surveillance, and (b) the manner in which that authority reviews surveillance requests and authorises surveillance.

– *Standard procedure*

307. When in 2007 it reviewed the authorisation procedure under the 1997 Act, the Court found that, if strictly adhered to, that procedure provided substantial safeguards against arbitrary or indiscriminate surveillance (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 84). The sophistication of the relevant provisions has since then grown (compare paragraphs 32 to 51 and 70 to 78 above with *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, §§ 12-17). Those procedures, however, must be examined not simply as they exist on paper but also as they operate in practice, as far as that can be ascertained on the basis of reliable official sources (compare with *Roman Zakharov*, cited above, §§ 263 and 265).

308. The relevant legislation in Bulgaria lays down robust safeguards intended to ensure that secret surveillance is resorted to only when that is truly justified. First, only a limited number of authorities can request surveillance, within the spheres of their respective competencies (see paragraphs 32 to 36 above). Secondly, the law appears to provide for a form of internal review preceding the submission of surveillance applications: those made by executive authorities must originate from the head of the respective authority, and public prosecutors intending to make such applications must notify their hierarchical superiors (see paragraph 37

above). Thirdly and most importantly, surveillance may be authorised only by the competent court president or an expressly authorised deputy (see paragraphs 46 and 47 above). Lastly, the authority which carries out the surveillance must, before proceeding with it, scrutinise the surveillance application for incompatibility *ratione materiae* or obvious mistakes and, if it spots issues in those respects, refer the application back to the judge who authorised the surveillance for reconsideration (see paragraph 73 above).

309. By law, surveillance applications must be duly reasoned and set out both the grounds for the requested surveillance and its intended parameters (see paragraphs 39, 40 and 41 above). An application must, in particular, (a) refer to the circumstances giving cause to suspect that a relevant offence is being prepared or committed or has been committed (including when it comes to national security), (b) set out (except in relation to terrorist offences) the investigative steps already taken and the results of any previous inquiries or investigations, (c) explain (except in relation to terrorist offences) why the requisite intelligence cannot be obtained through other means or why such other means would entail exceptional difficulties, and (d) explain (except in relation to terrorist offences) why the intended duration of the surveillance is necessary (see paragraphs 39 (a), (b), (d) and (f), 40 (a), (b), (e) and (f), and 41 (a) above). All materials on which the application is based must either be enclosed with it from the outset (for applications made outside criminal proceedings), or made available to the competent judge upon request (for applications made in the course of criminal proceedings) (see paragraph 44 above). When examining the application, the judge must review whether all legal prerequisites are in place and rule by means of a reasoned decision (see paragraph 51 above). One possible shortcoming at that stage is that although surveillance-warrant proceedings must of necessity be conducted without notice to the persons intended to be placed under surveillance, the requesting authority is under no duty to disclose to the judge fully and frankly all matters relevant to the well-foundedness of its surveillance application, including matters which may weaken its case.

310. Nonetheless, in spite of this latter potential shortcoming, the Court's finding in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, § 84) that, if strictly adhered to, the authorisation procedure in Bulgaria provides substantial safeguards against arbitrary or indiscriminate surveillance can only be confirmed. But it must also be seen whether those safeguards are being properly applied in practice.

311. The two courts in Bulgaria which have issued the highest number of surveillance warrants during the past decade were, by a large margin, the Sofia City Court (until 2015) and the Specialised Criminal Court (since 2015) (see the table under paragraph 49 above). According to an official report published in early 2017, until April 2015 all judges in the Sofia City Court issuing surveillance warrants gave no reasons whatever for their

decisions, and in April-August 2015 gave, with few exceptions, only "blanket and generalised" reasons (see paragraph 59 (h) and (i) above). That is confirmed by the two 2012 and 2013 surveillance warrants issued by that court submitted by the applicants (see paragraph 61 above). It is true that after the scandal which erupted in 2015 in relation to the manner in which the Sofia City Court was processing surveillance applications (and which later led to the dismissal and criminal conviction of its president), the competent judges of that court began systematically giving reasons for their decisions to issue surveillance warrants (see paragraphs 56, 57 and 60 above). At about the same time, however, the number of surveillance applications addressed to that court sharply declined, and the largest number of such applications started being submitted to the Specialised Criminal Court (see the table under paragraph 49 above). Indeed, since 2018 the Specialised Criminal Court has been issuing roughly half of all surveillance warrants in Bulgaria (ibid.).

312. As is apparent from two recent judgments of the Specialised Criminal Court, about thirty surveillance warrants issued by its president and vice-presidents had completely blanket contents, were couched in terms which were general enough to be capable of relating to any possible surveillance application, and lacked any reference to the specific case to which they related except the number of the application (see paragraphs 64 and 65 above). There is no reason to think that those warrants were somehow exceptional and represent anything other than the normal practice in that court.

313. It can thus be concluded that no proper reasons have been given for the decisions to issue the vast majority of all surveillance warrants issued in Bulgaria in the past decade. This is of particular relevance as the contemporaneous provision of reasons is a vital safeguard against abusive surveillance (see *Dragojević v. Croatia*, no. 68955/11, §§ 88-101, 15 January 2015; *Dudchenko v. Russia*, no. 37717/05, §§ 97-98, 7 November 2017; and *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, §§ 137-41, 28 May 2019). This is because the provision of reasons, even if succinct, is the only way of ensuring that the judge examining a surveillance application has properly reviewed the application and the materials which support it, and has truly directed his or her mind to the questions whether the surveillance would be a justified and proportionate interference with the Article 8 rights of the person(s) against whom it will be directed, and of any person(s) likely to be collaterally affected by it. In Bulgaria, that is particularly important in view of the applicants' allegation – which seems corroborated by, *inter alia*, some recent developments (see paragraph 67 above) – that criminal proceedings can be opened in a frivolous and abusive manner, chiefly with a view to making it possible to place someone under surveillance for ulterior motives (see paragraph 279 above). As demonstrated by the arrangements in the

Sofia City Court since August 2015, the provision of reasons, regardless of whether a surveillance application is allowed or refused, is not unachievable in practice, in spite of the fairly short time-limits for ruling on such applications (see paragraph 60 above).

314. It is true that, as noted in the two above-mentioned judgments of the Specialised Criminal Court (see paragraphs 64 and 65 above), the absence of reasons cannot automatically lead to the conclusion that the judges issuing surveillance warrants have not properly reviewed the applications for them. But three factors raise serious misgivings in that respect.

315. The first such factor is the sheer workload entailed by such applications, which by law can only be dealt with by the presidents or vice-presidents of the respective courts. The National Bureau has repeatedly drawn attention to the inadequate staff and resources placed at the disposal of the Specialised Criminal Court to process properly all surveillance applications submitted to its president and vice-presidents (see paragraph 50 above). The Specialised Criminal Court has itself also drawn attention to the ever-increasing workload entailed by the large volume of surveillance applications submitted to it (see paragraphs 62 and 63 above), and the issue has already been highlighted by the Committee of Ministers in the context of its supervision of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 229 (b) above).

316. The second factor is the high percentage of surveillance applications which are being allowed (see the table under paragraph 55 above).

317. The third factor is the express position of the Specialised Criminal Court of Appeal – which has direct supervisory jurisdiction over the Specialised Criminal Court – that a judge dealing with a surveillance application need only check whether the formal requirements to allow it are satisfied, without engaging with the materials in support of the application (see paragraph 66 above).

318. All of the above cannot be dismissed as a mere technicality which does not reflect on the substantive operation of the system of secret surveillance in Bulgaria. There is evidence which tends to suggest that the manner in which the competent judges go about examining surveillance applications has resulted in actual instances of unjustified surveillance.

319. First, the president of the Sofia City Court was dismissed in connection with the manner in which she had organised the processing of such applications in that court at the time when it was the court in Bulgaria which was issuing the highest number of surveillance warrants (see paragraph 57 above). She was also criminally convicted of deliberately authorising surveillance in breach of the statutory requirements (see paragraph 56 above). Although no such charges have been laid against other

judges of the Sofia City Court, there is evidence that the problem was far more generalised (see paragraphs 58 and 59 (c), (d), (e), (f) and (g) above).

320. As for the Specialised Criminal Court, it is noteworthy that in July 2021 the Bulgarian Parliament created an *ad hoc* committee to investigate the possibly unlawful and unjustified use of special means of surveillance with respect to opposition politicians, journalists, and hundreds of participants in the 2020 anti-government protests in Bulgaria, on the basis of warrants issued by that court. Although that committee's report, which was finalised in September 2021, is not yet publicly available, the statements which the Minister of Internal Affairs made in Parliament at the time when the committee was being set up already suggest that the problem with the absence of proper judicial scrutiny has seriously affected the surveillance operations authorised by the Specialised Criminal Court (see paragraph 67 above).

321. It follows that the Court cannot be satisfied that the procedures for authorising secret surveillance, as operating in practice in Bulgaria, effectively guarantee that such surveillance is authorised only when genuinely necessary and proportionate in each case (compare with *Roman Zakharov*, cited above, §§ 262-63).

322. The additional vetting carried out by the surveillance authorities after the grant of judicial authorisation (see paragraph 73 above) cannot remedy that lack of proper judicial scrutiny, for two reasons. First, that vetting is limited to incompatibility *ratione materiae* or obvious mistakes (ibid.). Secondly, the instances in which that additional safeguard has been triggered are apparently extremely rare (see paragraph 75 above).

– *Urgent procedure*

323. By contrast, it does not appear that a discrete issue arises with regard to the urgent procedure, under which special means of surveillance may be deployed without a prior judicial warrant if there is an immediate risk that a serious intentional offence is about to be committed, or a risk of an immediate threat to national security (see paragraph 77 above). When the authorities resort to that urgent procedure, the competent judge must within twenty-four hours assess and approve retrospectively the need for them to have done so; otherwise the surveillance operation must stop. The judge is not required to just review the need to pursue the surveillance, but must also validate the surveillance which has already taken place, as well as its results (contrast *Roman Zakharov*, cited above, § 266, and *Konstantin Moskalev v. Russia*, no. 59589/10, §§ 51-52, 7 November 2017). There have moreover been few instances in which that procedure has been used, and in 2018-20 those even diminished to a negligible percentage (see paragraph 78 above).

(ε) Procedures for storing, accessing, examining, using, communicating and destroying surveillance data

– *In general*

324. In *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, § 86), the Court found that there was an apparent lack of regulations specifying with an appropriate degree of precision the manner of screening of the information obtained through secret surveillance, or the procedures for preserving its integrity and confidentiality and its destruction.

325. The 1997 Act and the Code of Criminal Procedure have since then been amended, and now contain provisions dealing with various aspects of those issues. Lacunae remain, however, in several areas.

326. First, while those provisions specify the way in which information from the "primary recording" is to be reproduced in the "derivative data carrier" and then in any evidentiary material (see paragraphs 87 to 91 above), they say nothing about the way in which the "primary recording" and the "derivative data carrier" are to be stored. Nor do they circumscribe in any way the officials within the relevant authorities who are entitled to access them, or lay down any safeguards ensuring the integrity and confidentiality of those materials. It must be noted in this connection that since the repeal in August 2013 of point 8 of part II of Schedule no. 1 to the Protection of Classified Information Act 2002, information obtained by using special means of surveillance is no longer classified (see paragraph 102 above). It is thus apparently not subject to the rules governing the protection of such information – although the Technical Operations Agency maintained that despite the amendment both the "primary recording" obtained as a result of surveillance and the "derivative data carrier" remained classified information (see paragraph 104 above). As noted in paragraph 296 above, the internal rules to which the Government referred (see paragraphs 283 and 288 above) have not been published. They were not even disclosed in these proceedings (compare with *Big Brother Watch and Others*, cited above, § 423).

327. Moreover, aside from the general rule that the content of the "derivative data carrier" must fully match that of the "primary recording" (see paragraph 89 *in fine* above), no publicly available rules exist about the way in which the "primary recording" and the "derivative data carrier" are to be examined: how the authorities are to sift through the information in them and decide which parts are relevant and are to be kept and used as evidence, and which parts are irrelevant and are to be discarded. Although the rules governing the possible use of materials obtained as a result of secret surveillance say that any such materials, including surplus information, can be used only to prevent, detect or prove serious intentional criminal offences, or to protect national security (see paragraphs 18, 84, 100

and 101 above), it is thus unclear how compliance with that limitation is ensured in practice.

328. The rules governing the destruction of the "primary recording" and the "derivative data carrier" appear sufficiently clear, although a discrepancy exists between the position in relation to materials obtained as a result of surveillance outside the framework of already pending criminal proceedings and the position in relation to materials obtained in the course of criminal proceedings: the law provides for automatic destruction and subsequent report to the judge who has authorised the surveillance in the former case, and for a report to that judge and destruction by his or her order in the latter case (see paragraphs 94 to 99 above).

329. There are, however, no special rules about the storage or destruction of the resulting evidentiary material. At least two copies of that evidentiary material are produced in each case (which appear to consist in computer files containing audio- or video-recordings – see paragraph 90 above) and of the written records which accompany them (see paragraph 91 above). The first copy is sent to the judge who has issued the surveillance warrant (ibid.). The second copy is kept first by the requesting authority and then, if criminal proceedings are opened in connection with it, it is transferred to the case file of those proceedings – first the case file kept by the prosecuting authorities and then the case file kept by the criminal court(s) (see paragraph 92 above). It appears that both copies are stored and destroyed together with the case files of which they form part. It cannot be accepted that this provides an appropriate level of protection for information which may concern intimate aspects of someone's private life or otherwise permit a disproportionate invasion into the privacy of the people concerned or in the "correspondence" of any legal persons concerned. The scenario in which no criminal proceedings are opened also throws up many uncertainties.

330. Nor are there any publicly available rules governing the storage of information obtained through surveillance on national-security grounds – which must be kept by the relevant requesting authority for fifteen years after the end of the surveillance (see paragraph 98 above).

331. The Government did not argue that all or some of the above gaps have been filled by the provisions added in 2019 to the 2002 Act to transpose Directive (EU) 2016/680 (see paragraph 219 above), and it is unclear whether the competent authorities have regard to those data-protection rules when processing information obtained as a result of secret surveillance. Moreover, those rules cannot provide a safeguard with respect to information relating to legal persons (see paragraphs 216 and 239 above).

332. The apparent lack of clear regulation in all these fields, and of proper safeguards, makes it possible for information obtained as a result of secret surveillance to be misused for ends which have little to do with the statutory purpose.

– *With regard to surveillance affecting legal professional privilege*

333. A further issue in this regard arises from the absence of legal provisions specifying with an appropriate degree of precision the fate of information resulting from secret surveillance which may have affected materials subject to legal professional privilege. It is open to question whether the Chief Prosecutor's instruction on the point, which was a purely internal act issued pursuant to his power to make instructions governing the work of the prosecuting authorities (see paragraphs 27 above), can be seen as "law" for the purposes of Article 8 § 2 of the Convention (see, *mutatis mutandis*, *Silver and Others v. the United Kingdom*, 25 March 1983, § 86, Series A no. 61; *Malone v. the United Kingdom*, 2 August 1984, §§ 68 and 79, Series A no. 82; and *Amann v. Switzerland* [GC], no. 27798/95, § 75, ECHR 2000-II). It is moreover doubtful whether that instruction lays down sufficient safeguards in respect of secret surveillance directed against lawyers, since it simply makes this subject to the existence of a reasonable suspicion that they have committed an offence (see paragraph 28 above), which is in principle a requirement for all surveillance, not just that directed against lawyers (see paragraphs 39 and 54 above). The instruction also seems to contradict the express terms of section 33(1), (2) and (3) of the Bar Act 2004, according to which all lawyers' records and communications, regardless of their form, are privileged without exception (see paragraph 26 above). Nor does the instruction lay down enough safeguards with respect to materials obtained as a result of accidentally intercepted lawyer-client communications (see, *mutatis mutandis*, *R.E. v. the United Kingdom*, no. 62498/11, §§ 138-41, 27 October 2015, and *Dudchenko v. Russia*, no. 37717/05, § 107, 7 November 2017). Its only provision dealing with the issue, point 13, simply says that if the authorities intercept the conversation of a lawyer with a client or with another lawyer, and that conversation touches upon a client's defence, they must not prepare evidentiary material on its basis, unless the surveillance reveals that the lawyer has him- or herself engaged in criminal activity (see paragraph 29 above). That leaves open the question how precisely any such intercept materials are to be destroyed, as expressly required by section 33(3) of the Bar Act 2004 (see paragraph 26 above). Nor does the instruction appear to encompass all sorts of lawyer-client communications: by its terms, point 13 of the instruction applies solely to communications relating to a client's defence, which implies already pending litigation, and perhaps even just criminal proceedings.

(στ) Oversight arrangements

334. The relevant factors for deciding whether the oversight arrangements are adequate are (a) the independence of the supervisory authorities, their competences, and their powers (both to access materials

and to redress breaches, in particular order the destruction of surveillance materials), and (b) the possibility of effective public scrutiny of those authorities' work.

335. In Bulgaria, three authorities can supervise the use of special means of surveillance: (a) the judge who has issued the respective surveillance warrant; (b) the National Bureau; and (c) a special parliamentary committee (see paragraphs 106 to 135 above).

336. That system's sophistication goes well beyond the arrangements condemned by the Court in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, §§ 87-88). It nevertheless falls short of the requisite standard of effectiveness in several respects.

337. The judge who has issued the surveillance warrant is not in a position to ensure effective oversight. It is true that he or she must be informed of the end of the respective surveillance operation (see paragraphs 105 and 107 above, and contrast *Roman Zakharov*, cited above, § 274), and given a report about it (see paragraph 106 above). But in all instances of surveillance outside already pending criminal proceedings that judge has no power to order remedial measures, such as the destruction of surveillance materials. More importantly, he or she is not empowered or expected to carry out on-site inspections, and performs his or her supervisory duties solely on the basis of the report submitted by the authorities. Also, in view of the high workload of the judges concerned (see paragraph 315 above), it is open to doubt whether that supervision could be effective in practice. In sum, although a valuable safeguard, that mechanism is insufficient to ensure that surveillance powers are not being abused.

338. For its part, the main supervisory body, the National Bureau, suffers from several shortcomings undermining its effectiveness in practice.

339. First, there is no guarantee that all of its members are sufficiently independent *vis-à-vis* the authorities which they must oversee. By law, individuals with professional experience in the law-enforcement or the security services may become members of the National Bureau (see paragraph 109 above). After serving their five-year term (which, granted, can be renewed), they are entitled to regain their previous posts (see paragraph 111 above). This potential "revolving door" mechanism can raise misgivings about the practical independence of such members of the Bureau and about possible conflicts of interests on their part (see, *mutatis mutandis*, *Centrum för rättvisa*, cited above, § 359). Indeed, the Bureau's current chairperson came directly from the State Agency for National Security, and the deputy chairperson who was elected in 2018 and resigned in mid-2021 (after having been placed under sanctions by the authorities of the United States of America on serious corruption allegations) had been employed by the security services for more than two and a half decades before joining the Bureau (see paragraphs 112 and 115 above).

340. Another aspect of the National Bureau's organisation raises further misgivings in this respect. Before being appointed to their posts, its members must undergo security vetting by one of the very authorities whose work the Bureau is overseeing – the State Agency for National Security (see paragraphs 109 and 110 above). This creates an obvious conflict of interests for that Agency. If it later revokes the security clearance of members of the Bureau, they must be removed from their post since they automatically cease being eligible to occupy it; that already happened once in 2017-18 (see paragraphs 111 (c) and 114 above). Although the Agency's decision to revoke a security clearance is amenable to judicial review, that possibility for it to influence the Bureau's membership is capable of affecting the Bureau's independence and the objectivity and thoroughness of its supervisory work, especially with regard to that Agency.

341. The issue with the National Bureau's independence *vis-à-vis* the authorities which it oversees has already been highlighted by the Committee of Ministers of the Council of Europe in the context of its supervision of the execution of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 229 (e) above).

342. Secondly, misgivings arise about the qualifications of some of the members of the National Bureau. Only one of its current five members has legal training and experience (see paragraph 112 above, and contrast *Big Brother Watch and Others*, cited above, § 407). This point has also been noted by the Committee of Ministers (see paragraph 229 (e) above).

343. Thirdly, it does not appear that when carrying out on-site inspections members of the National Bureau and its employees are able to have unfettered access to all relevant materials held by the prosecuting authorities and the State Agency for National Security, especially materials enabling them to check the well-foundedness of surveillance applications (reasonable suspicion and proportionality in each case) (see paragraphs 118 and 119 above). The Bureau has also complained of the repeated provision of incorrect information by the main surveillance authority in Bulgaria, the Technical Operations Agency (see paragraph 118 *in fine* above). Such obstruction seriously weakens the Bureau's oversight capabilities, and cannot be seen as justified (compare, *mutatis mutandis*, with *Roman Zakharov*, cited above, § 281). Providing Bureau members with access to all materials in the case file of a criminal case cannot prejudice ongoing investigations since those members have the highest security clearance and are bound by professional secrecy (see paragraphs 109, 110 and 129 above). The Committee of Ministers has already drawn attention to that issue as well (see paragraph 229 (e) above).

344. Lastly, the National Bureau has no power to order remedial measures, such as the destruction of surveillance materials. It can only bring irregularities to the attention of the heads of the relevant authorities and the prosecuting authorities, or of the Supreme Judicial Council, for irregularities

attributable to judges (see paragraphs 122 and 123 above). The Bureau's power to give instructions appears to relate solely to instructions intended to improve practices rather than instructions in specific cases, as attested in particular by their limited number per year (see paragraphs 120 and 121 above).

345. The special parliamentary committee is not empowered to order remedial measures either (see paragraph 127 above). Moreover, unlike the National Bureau, it does not appear to conduct regular inspections (see paragraph 128 above and compare with the table under paragraph 124 above).

346. The Government did not argue, and there is no indication, that the Commission for Protection of Personal Data or the Inspectorate attached to the Supreme Judicial Council have so far played any role in the oversight of the system of secret surveillance by virtue of their powers under 2002 Act, as amended in 2019 to transpose Directive (EU) 2016/680 (see paragraphs 225 and 226 above).

347. In view of the defects outlined above, the system of overseeing secret surveillance in Bulgaria as it is currently organised does not appear capable of providing effective guarantees against abusive surveillance.

(ζ) Notification

348. The relevant factors under this rubric are (a) when is such notification possible, and (b) whether it is a prerequisite for using the available remedies.

349. As already noted in paragraph 267 above, the National Bureau must notify someone who has been placed under secret surveillance only if that has happened unlawfully, whereas under the Court's case-law such notification is, in the absence of a remedy available without prior notification, required in all cases, as soon as it can be made without jeopardising the purpose of the surveillance (see *Klass and Others v. Germany*, 6 September 1978, § 58, Series A no. 28; *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 135, ECHR 2006-XI; and, more recently, *Roman Zakharov*, cited above, § 287). It is telling in that respect that the number of notifications made by the Bureau each year relative to the annual number of surveillance warrants is very small (compare the tables under paragraphs 55 and 135 above). Moreover, the Bureau is only required to notify individuals, not legal persons (see paragraph 130 above) – a point already noted by the Committee of Ministers in the context of its supervision of the execution of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 229 (e) *in fine* above).

350. The Government did not argue, and there is no indication, that there have so far been instances in which such notification has been made by virtue of section 54(4) of the 2002 Act, as amended in 2019 to transpose

Directive (EU) 2016/680 (see paragraph 220 above). Nor does it appear that there have so far been any instances in which people have been able to obtain information about secret surveillance under section 55(3) *in fine*, section 56(6) *in fine* or section 57(1) and (2) of the same Act, as worded after the 2019 amendment (see paragraphs 221 and 224 above).

351. At the same time, as already noted in paragraphs 266 to 271 above, notification by the National Bureau is normally a prerequisite to bringing a claim for damages under section 2(1)(7) of the 1988 Act; the only other situation in which such a claim may become available is when the secret surveillance has come to light because the materials from it have been used in criminal proceedings.

(η) Remedies

352. In 2009 Bulgaria put in place a dedicated remedy in respect of secret surveillance: a claim for damages under section 2(1)(7) of the 1988 Act (see paragraph 136 above). But that remedy, although effective in some scenarios, suffers from three serious limitations outlined in paragraphs 266 to 273 above: (a) it has so far not been able to operate in the absence of prior notification by the National Bureau that someone has been placed under surveillance, (b) it does not entail an examination of the necessity for the surveillance in each case, and (c) it is not open to legal persons.

353. Moreover, the only form of relief available in such proceedings is money damages (see paragraph 139 above); the courts have no power to order the destruction of surveillance material (contrast, for instance, *Big Brother Watch and Others*, cited above, § 413). The Committee of Ministers has already highlighted this point in the context of its supervision of the execution of *Association for European Integration and Human Rights and Ekimdzhiev* (cited above) (see paragraph 229 (f) *in fine* above).

354. As noted in paragraph 275 above, the novel remedies available under the 2002 Act, as amended in 2019 to transpose Directive (EU) 2016/680 (see paragraphs 221, 224 and 227 above), have so far not been shown to be effective in relation to secret surveillance, and are moreover not available to legal persons.

355. It follows that Bulgarian law does not provide an effective remedy to all persons suspecting, without concrete proof, that they have been unjustifiably subjected to secret surveillance. It also follows that the Government's objection that domestic remedies have not been exhausted, which was joined to the merits (see paragraph 259 above), must be rejected.

(θ) Conclusion

356. Although significantly improved after they were examined by the Court in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above), the laws governing secret surveillance in

Bulgaria, as applied in practice, still fall short of the minimum safeguards against arbitrariness and abuse required under Article 8 of the Convention in the following respects:

(a) the internal rules governing the storage and destruction of materials obtained via surveillance have not been made accessible to the public (see paragraph 296 *in fine* above);

(b) the term "objects" in section 12(1) of the 1997 Act is not defined in a way so as ensure that it cannot serve as a basis for indiscriminate surveillance (see paragraph 303 above);

(c) the excessive duration of the initial authorisation for surveillance on national-security grounds – two years – significantly weakens the judicial control to which such surveillance is subjected (see paragraph 305 above);

(d) the authorisation procedure, as it operates in practice, is not capable of ensuring that surveillance is resorted to only when "necessary in a democratic society" (see paragraphs 307 to 322 above);

(e) a number of lacunae exist in the statutory provisions governing the storing, accessing, examining, using, communicating and destroying of surveillance data (see paragraphs 326 to 332 above);

(f) the oversight system, as currently organised, does not comply with the requirements of sufficient independence, competence and powers (see paragraphs 335 to 347 above);

(g) the notification arrangements are too narrow (see paragraphs 349 to 351 above); and

(h) the dedicated remedy, a claim under section 2(1)(7) of the 1988 Act, is not available in practice in all possible scenarios, does not ensure examination of the justification of each instance of surveillance (by reference to reasonable suspicion and proportionality), is not open to legal persons, and is limited in terms of the relief available (see paragraphs 266 to 273 and 352 to 355 above).

357. Those shortcomings in the legal regime appear to have had an actual impact on the operation of the system of secret surveillance in Bulgaria. The recurring scandals relating to secret surveillance (see paragraphs 56, 57, 59 and 67 above) suggest the existence of abusive surveillance practices, which appear to be at least in part due to the inadequate legal safeguards (see *Association for European Integration and Human Rights and Ekimdzhiev*, § 92, and *Roman Zakharov*, § 303, both cited above).

358. It follows that the Bulgarian laws governing secret surveillance do not fully meet the "quality of law" requirement and are incapable of keeping the "interference" entailed by the system of secret surveillance in Bulgaria to what is "necessary in a democratic society".

359. There has therefore been a breach of Article 8 of the Convention.

II. RETENTION AND ACCESSING OF COMMUNICATIONS DATA

360. The applicants also complained that the system of retention and subsequent accessing of communications data in Bulgaria did not meet the requirements of Article 8 of the Convention, and that they did not have an effective remedy in that respect, in breach of Article 13 of the Convention.

361. In the light of the Court's case-law (see *Roman Zakharov*, cited above, § 307), this complaint likewise falls to be examined solely under Article 8 of the Convention, whose text, so far as relevant, has been set out in paragraph 247 above.

A. Admissibility

1. The parties' submissions

(a) Victim status of the applicants

(i) The Government

362. The Government submitted that the applicants could not claim to be victims of a violation of their right to respect for their private life or correspondence. That was because under Bulgarian law communications data could be accessed only in connection with serious criminal offences, even when national security was at stake. Moreover, since in Bulgaria legal persons could not bear criminal liability, the two applicant organisations were outside the scope of the contested laws.

363. The Government went on to argue that the applicants, who all had the requisite legal expertise, could have urged the special parliamentary committee to check whether their retained communications data had been accessed unlawfully. That committee was also bound to inform individuals of unlawful requests for access, or access, of their communications data on its own initiative. Individuals could also seek information on the point under the 2002 Act – which, as amended in 2019, had transposed Directive (EU) 2016/380 – or under the GDPR, from the communications service providers themselves or from the Commission for Protection of Personal Data. The notification procedure was coupled with possibilities to complain to that Commission and seek damages from the communications service providers or from the relevant authorities under the relevant provisions of the 2002 Act or the general law of tort. Since those remedies were effective, the applicants' failure to use them stripped them of their victim status and rendered their complaint an *actio popularis*.

(ii) The applicants

364. The applicants argued that in view of the similarities between secret surveillance and the retention and subsequent accessing of communications data, the approach to the question whether they could claim to be victims of

interference with their rights under Article 8 of the Convention on account of the latter had to be the same as the one taken by the Court with respect to the former. They all used electronic communications services, and the laws in issue applied to all such users, including legal persons. The fact that those laws enabled the authorities to access retained data only in connection with serious criminal offences – a rule which had in any event been flouted on several reported occasions – did not detract from that position, especially in the light of the many thousands of access applications in each of the recent years and the feeble oversight arrangements. The applicants further underlined that the retained data enabled the profiling of all persons in the country. Its unlawful use in disciplinary proceedings against judges and prosecutors in 2010-11 had amply illustrated the potential for abuse.

365. Bulgarian law did not lay down effective procedures whereby the applicants could obtain information about the retention or accessing of their communications data or compensation in respect of that. They could hence claim to be victims of a violation owing to the mere existence of laws permitting the retention and accessing of communications data.

(b) Exhaustion of domestic remedies

366. Based on the arguments summarised in paragraph 363 above, the Government further submitted that the applicants had not exhausted domestic remedies.

367. The applicants disputed that assertion, noting that when they had lodged their application, neither the Commission for Protection of Personal Data nor the special parliamentary committee had had any functions relating the retention or accessing of communications data. It had therefore not been open to them to complain to either of those authorities about the matter.

2. The Court's assessment

368. Similarly to the position in relation to the complaint about secret surveillance (see paragraph 259 above), both of the Government's objections are so closely linked to the substance of the applicants' complaint that they must be joined to the merits.

369. The complaint is, moreover, not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention or inadmissible on other grounds. It must therefore be declared admissible.

B. Merits

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

(a) The parties' submissions

370. The parties' submissions have been summarised in paragraphs 362 to 365 above.

(b) The Court's assessment

371. Under Bulgarian law, all communications service providers in the country must retain all the communications data of all of their users for six months, with a view to making that data available to the authorities for certain law-enforcement purposes (see paragraphs 161 and 163 above). Various authorities may then access that data (see paragraphs 167 to 169 above). It is appropriate to analyse those two steps separately, since each of them may affect the rights guaranteed under Article 8 of the Convention in different ways and to different degrees (see, *mutatis mutandis*, *Centrum för rättvisa*, §§ 239-43, and *Big Brother Watch and Others*, §§ 325-29, both cited above).

(i) Retention of communications data by communications service providers

372. It is settled that the mere storing of data relating to someone's private life amounts to interference with that individual's right to respect for his or her "private life" (see, with respect to personal data relating to the use of communications services, *Breyer v. Germany*, no. 50001/12, § 81, 30 January 2020; *Centrum för rättvisa*, cited above, § 244, and *Big Brother Watch and Others*, cited above, § 330). All types of communications data at issue in the present case – subscriber, traffic and location data – can relate, alone or in combination, to the "private life" of those concerned. Bulgarian law requires all communications service providers in the country to retain the entirety of that data of all users for potential subsequent access by the authorities (see paragraph 161 above). It has not been disputed that the two individual applicants use such services. It follows that this legally mandated retention is in itself an interference with their right to respect for their "private life", irrespective of whether the retained data are then accessed by the authorities.

373. That retention amounts also to interference with those applicants' right to respect for their correspondence. The Court has already held that the storage of traffic and location data relating to a mobile telephone line amounts to interference with the right of the person using that line to respect for his "correspondence" (see *Ben Faiza v. France*, no. 31446/12, §§ 66-67, 8 February 2018). There is no reason to hold otherwise with respect to other types of communications, such as electronic communications, or with respect to communications data more generally.

374. As for the two applicant organisations, it is settled that the communications of legal persons are covered by the notion of "correspondence" in Article 8 § 1 of the Convention (see *Association for European Integration and Human Rights and Ekimdzhiev*, § 60, and *Liblik and Others*, § 110, both cited above). It has not been disputed that the two organisations likewise use communications services in Bulgaria. It follows that the legally mandated retention of the communications data of all users

of communications services in the country is interference with their right to respect for their "correspondence".

375. The interference, although carried out by private persons – the communications service providers – is required by law. Indeed, service providers who fail to comply with their statutory data-retention obligations are liable to sanctions (see paragraph 161 *in fine* above). It follows that the interference is attributable to the Bulgarian State (compare with *Digital Rights Ireland and Others*, cited in paragraph 233 above, § 34).

(ii) Accessing of retained communications data by the authorities

376. Access by the authorities to the retained communications data constitutes a further interference with right to respect for one's private life and one's communications under Article 8 of the Convention (see, *mutatis mutandis*, *Centrum för rättvisa*, § 244, and *Big Brother Watch and Others*, § 330, both cited above). But it is plain that not all retained communications data is subsequently accessed by the authorities. Since it is impossible for an individual or a legal person to know for certain whether their data has been so accessed, it is appropriate to analyse the question whether the applicants may claim that they are victims of interference with their rights under Article 8 owing to the mere existence of laws permitting authorities to do so with reference to the same criteria as the ones used in relation to secret surveillance: (a) the scope of the laws permitting such access and (b) the availability of an effective remedy (see paragraphs 262 to 275 above).

(α) Scope of the relevant law

377. Under the relevant statutory provisions, the authorities may access the retained communications data of anyone if that is necessary for (a) national-security purposes; (b) the prevention, detection or investigation of serious criminal offences; (c) the tracing of people who have been finally sentenced to imprisonment with respect to a serious criminal offence or who have fallen or could fall in a situation which puts their life or health at risk; and (d) (this applies solely to cell ID) the carrying out of search-and-rescue operations with respect to people in distress (see paragraph 163 above). Since the communications data of anyone in Bulgaria can theoretically become necessary for one or more of those purposes, all four applicants, including the applicant organisations, can possibly be affected by the contested legislation.

(β) Availability of an effective remedy

378. The next question is whether there exists an effective remedy which can alleviate the suspicion among the general public that retained communications data is being abusively accessed and used.

379. Neither the 2007 Act nor Article 159a of the Code of Criminal Procedure provide for a remedy with respect to the retention or accessing of communications data.

380. Nothing suggests that the remedies under section 38(1) and (7), section 39(1) and (2), and section 82(1) of the 2002 Act, as worded after the 2019 amendment intended to transpose Directive (EU) 2016/680 (see paragraphs 218 and 227 above), have so far been used to provide redress with respect to the retention of communications data by communications service providers or with respect to its accessing and use by the authorities. In the absence of reported decisions by the Bulgarian courts, it is not for this Court to say whether or how those remedies, which are general in application, can operate in such cases. It is true that those remedies are novel, and that they are part of a branch of law which has only developed relatively recently. But it was for the Government to explain their manner of operation, and as far as possible support their explanations with concrete examples (see, *mutatis mutandis*, *Roman Zakharov*, § 295, and *Mustafa Sezgin Tanrıkulu*, §§ 28-29, both cited above). The Government were, however, vague on the point, contenting themselves to say that the 2019 amendment had introduced provisions governing the liability of communications service providers and the relevant authorities in respect of retained and accessed communications data (see paragraphs 363 and 388 above, and contrast the circumstances in *Ringler v. Austria* (dec.) [Committee], no. 2309/10, §§ 12-13 and 51-54, 15 May 2020). In the absence of further particulars about the actual operation of those remedies with respect to communications data, it cannot be accepted that they are currently effective in that respect. Moreover, those remedies are not open to legal persons (see paragraphs 216 and 239 above).

381. Nor is there any evidence that a remedy is available under the general law of tort.

382. It follows that the public's misgivings about the threat of abusive accessing and use of communications data by the authorities cannot be sufficiently dispelled by the presence of effective remedies in that respect.

(γ) Conclusion

383. In view of the above considerations, there is no need to inquire whether the applicants are at risk of having their retained communications data accessed by the authorities owing to their personal situation (see, *mutatis mutandis*, *Centrum för rättvisa*, cited above, §§ 175-76).

384. It follows that an examination of the laws governing the accessing of retained communications data by the authorities in the abstract is justified. It also follows that the Government's objection that the applicants may not claim to be victims of a violation of Article 8 of the Convention allegedly caused by the mere existence of such laws, which was joined to the merits (see paragraph 368 above), must be rejected.

2. Justification for the interference

(a) The parties' submissions

(i) The applicants

385. The applicants submitted that the manner in which the law regulated the authorisation of access to communications data – in particular, the lack of any requirement for the authority seeking access to provide evidence in support of its application – did not ensure enough guarantees against abuse. There was, moreover, no requirement for ongoing judicial oversight. The publicly available judicial decisions on access applications, many of which contained only stereotyped reasoning, showed that judicial control in such cases was formal and provided few guarantees against abuse.

386. The remaining oversight arrangements were likewise insufficient. The special parliamentary committee was under no duty to examine individual complaints, and there were no publicly available rules governing its work. It was hence unsurprising that although the authorities made tens of thousands of requests for access to retained communications data each year, that committee had so far received only between one and four complaints annually. Even so, the committee's reports had recorded worrying breaches of the law. For its part, the Commission for Protection of Personal Data was simply gathering statistics about the retention of communications data. Its reports did not mention any instances in which it had examined individual complaints, and it was unclear how the GDPR could come into play in connection with that.

387. Moreover, the law did not require notification in cases of lawful access to retained communications data. That was a serious deficiency since the way in which the lawfulness of the access in each case was being assessed remained unclear. In practice that meant that if a court had issued an access warrant, those concerned would then not be notified of the access and would thus be unable to use any remedies in relation to it. Claiming damages under the GDPR was impossible, since it did not apply to data processing by the authorities for law-enforcement purposes. Unlike the position with respect to secret surveillance, the 1988 Act did not envisage liability of the courts or the prosecuting authorities in connection with retained communications data. But even if the law had made it possible to claim damages in this context, it would in practice be hard for individuals or legal persons alike to show non-pecuniary damage on account of such matters since they could not prove that an action of which they had remained unaware had caused them negative emotions. Pecuniary damage was, for its part, nearly impossible to establish. To be effective, a remedy in that domain had to address those points, for instance by providing for lump-sum compensation.

(ii) The Government

388. The Government submitted that the law specified clearly what communications data was to be retained, for how long, and for what purposes. A 2019 amendment implementing the GDPR and Directive (EU) 2016/680 had brought in stringent data-protection safeguards and provisions governing the liability of communications service providers and the authorities, and had expanded the powers of the supervisory authorities. The relevant rules were foreseeable and contained enough safeguards against arbitrariness.

389. This type of data retention was done in the interests of national security and public safety, and for the prevention of crime.

390. As for its necessity, there was no European consensus about the need to retain communications data or its modalities. Even after the CJEU's judgments in *Digital Rights Ireland and Others* and *Tele2 Sverige and Watson and Others* (see paragraphs 233 and 240 above), many member States of the European Union had not fully repealed their laws providing for the generalised retention of communications data, since that was a valuable instrument for combatting serious crime. A more restrictive approach could prevent the proper operation of that instrument. The CJEU had not altogether dismissed the importance of retaining communications data, and the matter remained within the States' margin of appreciation.

391. In Bulgaria, retained communications data could be accessed only in connection with serious offences and on the basis of a judicial warrant. The law set out in an exhaustive way the authorities which could seek such warrants, and required them to give enough reasons why they should be granted. If the materials in support of the warrant application were insufficient, judges could request further information, and their decisions in such cases were usually well reasoned. The possibility for communications service providers to refuse access to data retained by them if the necessary prerequisites were absent was an additional safeguard against abuse.

392. There were also clear rules on the destruction of retained data, and the judge who had issued an access warrant had to be informed of that destruction. The whole process was moreover overseen by the Commission for Protection of Personal Data and the special parliamentary committee.

393. Lastly, as regards notification arrangements and remedies, the Government referred to their submissions on the applicants' victim status (see paragraph 363 above).

(b) The Court's assessment

(i) General principles

394. In view of the technological and social developments in the past two decades in the sphere of electronic communications, communications data can nowadays reveal a great deal of personal information. If obtained

by the authorities in bulk, such data can be used to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who that person has interacted with (see *Centrum för rättvisa*, § 256, and *Big Brother Watch and Others*, § 342, both cited above). The acquisition of that data through bulk interception can therefore be just as intrusive as the bulk acquisition of the content of communications, which is why their interception, retention and search by the authorities must be analysed by reference to the same safeguards as those applicable to content (see *Centrum för rättvisa*, § 277, and *Big Brother Watch and Others*, § 363, both cited above).

395. Here, it must be added that by the same token, the general retention of communications data by communications service providers and its access by the authorities in individual cases must be accompanied, *mutatis mutandis*, by the same safeguards as secret surveillance (see paragraphs 291 to 293 above).

(ii) Application of those principles

(α) Accessibility of the law

396. All statutory provisions governing the retention of communications data and its accessing by the authorities have been officially published and are thus accessible to the public.

(β) Protection of retained data by communications service providers

397. Bulgarian law expressly requires that communications service providers store and process retained communications data in line with the rules governing the protection of personal data, and that various technical and organisational safeguards be put in place to ensure that such data is not unduly accessed, disclosed or altered, and that it is destroyed when the statutory period for its retention expires (see paragraphs 164 to 166 above).

(γ) Grounds on which retained data can be accessed by the authorities

398. In Bulgaria, the law sets outs in an exhaustive manner the grounds on which the authorities may seek access to retained communications data: protecting national security; preventing, detecting or investigating serious criminal offences; tracing people finally sentenced to imprisonment with respect to such offences; tracing people who have fallen or could fall into a situation which puts their life or health at risk; and (only as concerns location data) carrying out search-and-rescue operations with respect to people in distress (see paragraph 163 above). The law is thus sufficiently clear on that point. As noted in paragraph 301 above in relation to secret surveillance, the mere fact that one of the grounds for accessing retained

communications data is "national security" is not in itself contrary to Article 8 of the Convention.

399. It must also be noted in this connection that when in 2020 the Bulgarian Parliament broadened the possible grounds for acquiring retained communications data to include enforcement of isolation and quarantine measures in connection with infectious diseases, the Constitutional Court struck down the amendment as a whole, on the basis that it disproportionately interfered with the constitutional right to privacy (see paragraphs 158 and 159 above).

(δ) Procedure for obtaining access

– *Standard procedure*

400. Bulgarian law lays down safeguards intended to ensure that retained communications data is accessed by the authorities only when that is justified. First, only a limited number of authorities can seek access to that data, within the spheres of their respective competencies (see paragraphs 167 to 169 above). More importantly, such access can be granted only by the competent court president or by a judge to whom that power has been delegated (for access requested outside the framework of already pending criminal proceedings), or by a judge of the competent first-instance court (for access requested by a public prosecutor in the course of criminal proceedings) (see paragraphs 173 to 177 above).

401. Those safeguards nonetheless fall short of the requisite standard of effectiveness in several respects.

402. Access applications made outside the framework of already pending criminal proceedings must set out not only the grounds for seeking access to such data and the purpose for which it is being sought, but also contain a full account of the circumstances which show that the data is needed for a relevant purpose (see paragraph 171 above). By contrast, access applications made in the course of criminal proceedings, although expected to feature information about the alleged offence in connection with which access is being sought, are not expressly required to explain, in terms, why the data at issue is truly needed – they only have to contain a description of the circumstances underlying the access application, which appears to be an altogether looser requirement (see paragraph 172 above). The law does not therefore make it plain in all situations that access in each individual case can be sought and granted only if the resulting interference with the Article 8 rights of the person(s) concerned would be truly necessary and proportionate.

403. As with the procedure for authorising secret surveillance (see paragraph 309 *in fine* above), a further possible shortcoming at that stage is that although data-access proceedings must of necessity be conducted without notice to the persons whose communications data is being sought,

the authority seeking access is under no duty to disclose to the judge fully and frankly all matters relevant to the well-foundedness of its access application, including matters which may weaken its case.

404. The law does not require that supporting materials be enclosed with the access application either, which can in many cases prevent the judge who deals with the application from properly checking whether it is well-founded.

405. Nor does the law require judges examining such applications to give reasons explaining why they have decided that granting access to the communications data at issue was truly necessary (see paragraphs 179 and 180 above). As already noted in relation to the procedure for authorising secret surveillance (see paragraph 313 above), the provision of reasons, even if succinct, is the only way of ensuring that the judge examining an access application has properly reviewed the application and the materials which support it, and has truly directed his or her mind to the questions whether accessing the communications data at issue would be a justified and proportionate interference with the Article 8 rights of the person(s) whose data is being accessed, and any person(s) likely to be collaterally affected by that.

406. It follows that the procedures for authorising the authorities to access retained communications data do not effectively guarantee that such access is granted only when genuinely necessary and proportionate in each case.

– *Urgent procedure*

407. By contrast, it does not appear that a discrete issue arises with regard to the urgent procedure, under which the authorities may access retained communications data without a prior judicial warrant if there is an immediate danger that a terrorist offence will be committed (see paragraph 183 above). When the authorities resort to that urgent procedure, the competent judge must within twenty-four hours assess and approve retrospectively the need for them to have done so; otherwise any data made available pursuant to the direct-access request must be destroyed by the authority which has received it (see paragraphs 184 and 185 above). Moreover, that urgent procedure is apparently used sparingly (see paragraph 186 above, and compare it with the table under paragraph 182 above).

(ε) Amount of time for which the authorities may store and use accessed data not subsequently used in criminal proceedings

408. The 2007 Act says that any communications data not used to open criminal proceedings must be destroyed within three months of its receipt by the authorities, and that any data accessed under the urgent procedure must be immediately destroyed in the same way if resort to that urgent

procedure has not been retrospectively validated by the competent judge (see paragraphs 194 and 195 above). By contrast, no such time-limit has been laid down in relation to data accessed in the course of criminal proceedings. Although the point seems to be covered by internal rules issued by the Chief Prosecutor, those have not been made accessible to the public and it is unclear what they say (see paragraph 196 above). Nothing suggests that the provisions of the 2002 Act, as amended in 2019 to transpose Directive (EU) 2016/680 (see paragraph 219 above), have so far been used to fill that lacuna.

(στ) Procedures for storing, accessing, examining, using, communicating and destroying data accessed by the authorities

409. The 2007 Act and the Code of Criminal Procedure say nothing about the procedures for storing, accessing, examining, using, communicating and destroying communications data accessed by the authorities, and those points are not specifically covered by the rules governing prosecutorial and judicial case files either (see paragraph 193 above). It appears that such data is simply kept in the criminal case file, follows its fate, and can be accessed by anyone who can access the case file itself (ibid.). It cannot be accepted that this provides an appropriate level of protection for data which may sometimes concern intimate aspects of someone's private life or otherwise permit a disproportionate invasion into the privacy of the people concerned or in the "correspondence" of the legal persons concerned. Here also, nothing suggests that the provisions of the 2002 Act, as amended in 2019 to transpose Directive (EU) 2016/680 (see paragraph 219 above), have so far been used to fill that lacuna.

(ζ) Oversight arrangements

410. In Bulgaria, three authorities can oversee the retention of communications data and its subsequent accessing by the authorities: (a) the Commission for Protection of Personal Data; (b) the judge who has issued the access warrant; and (c) the same parliamentary committee which oversees secret surveillance (see paragraphs 197 to 210 above).

411. Under the 2007 Act, the Commission for Protection of Personal Data may (a) request communications service providers to provide it with any information relevant to its mandate in that domain, (b) check how those providers comply with their duties to communicate personal data breaches to users, and (c) check the technical and organisational measures taken by those providers to store retained communications data (see paragraphs 201 and 202 above). It may also give binding instructions to communications service providers and sanction them (see paragraphs 203 and 204 above). But its mandate under the 2007 Act appears to be limited to overseeing communications service providers (see paragraph 198 above); it has no

express powers under that Act with respect to the authorities which can access retained communications data.

412. It is true that under the provisions of the 2002 Act, as amended in 2019 to transpose Directive (EU) 2016/680, the same Commission – as well as the Inspectorate attached to the Supreme Judicial Council – are tasked with supervising the way in which the authorities process any personal data for law-enforcement purposes (see paragraph 225 above). But nothing suggests that either of those two authorities has so far availed itself of those powers in relation to communications data.

413. For his or her part, the judge who has issued the access warrant is not in a position to ensure effective oversight. Granted, he or she must be informed of the destruction of irrelevant or unhelpful communications data accessed by the authorities (see paragraph 197 above). But that judge has no power to order remedial measures. He or she is, moreover, not empowered or expected to carry out on-site inspections, and performs his or her supervisory duties solely on the basis of the report submitted by the authorities. Although a valuable safeguard, that mechanism is insufficient to ensure that data-accessing powers are not being abused.

414. The main supervisory body, the special parliamentary committee, can oversee both communications service providers and the relevant authorities (see paragraph 205 above), and has extensive information-gathering and inspection powers (see paragraph 207 above). Its annual reports demonstrate that it regularly carries out inspections via the experts it employs (see paragraphs 208 to 210 above). But several shortcomings undermine its effectiveness. First, its members need not be persons with legal qualifications or experience (see paragraph 206 above). Secondly, it has no power to order remedial measures in concrete cases, such as the destruction of retained or accessed communications data; it can only give instructions designed to improve the relevant procedures (see paragraph 211 above). If it detects irregularities, it can only bring the matter to the attention of the prosecuting authorities, or inform the heads of the relevant access-requesting authorities and communications service providers (see paragraph 212 above).

415. In view of the shortcomings outlined above, the system of overseeing the retention of communications data and its subsequent accessing by the authorities in Bulgaria, as currently organised, does not appear capable of providing effective guarantees against abusive practices in this respect.

(η) Notification

416. The 2007 Act requires the special parliamentary committee to notify an individual if his or her retained communications data has been accessed or sought to be accessed unlawfully, if such notification would not defeat the purpose for which those data has been accessed (see

paragraph 213 above). However, as noted in paragraph 349 above in relation to secret surveillance, under the Court's case-law such notification is required in all cases, not only those in which the data has been accessed unlawfully, as soon as the notification can be made without jeopardising the purpose of the measure.

417. Nothing suggests that such notification has so far been made by virtue of section 54(4) of the 2002 Act, as amended in 2019 to transpose Directive (EU) 2016/680 (see paragraph 220 above). Nor does it appear that there have so far been any instances in which people have been able to obtain information about the retention or accessing of their communications data under section 37a, section 55(3) *in fine*, section 56(6) *in fine* or section 57(1) and (2) of the same Act, as worded after the 2019 amendment (see paragraphs 217, 221 and 224 above). The Government were vague on the point, contenting themselves to say that the amendment had introduced provisions enabling individuals to obtain such information in respect of retained and accessed communications data (see paragraph 363 above, and contrast the circumstances in *Ringler*, cited above, §§ 12-13 and 51-54). In the absence of further particulars about the actual operation of those data-protection provisions with respect to retained communications data, it cannot be accepted that they are currently effective in that respect. Moreover, those information rights are not available to legal persons (see paragraphs 216, 234 and 239 above).

(θ) Remedies

418. As already noted in paragraphs 379 to 381 above, it has not been shown that an effective remedy exists in Bulgaria in respect of the retention and accessing of communications data. The Government's objection that the applicants have not exhausted domestic remedies in that respect, which was joined to the merits (see paragraph 368 above), must therefore be rejected.

(ι) Conclusion

419. Although the laws governing the retention of communications data and its subsequent accessing by the authorities were significantly improved after the Constitutional Court examined them in 2015 in the wake of the CJEU's judgment in *Digital Rights Ireland and Others* (see paragraph 156 above), those laws, as applied in practice, still fall short of the minimum safeguards against arbitrariness and abuse required under Article 8 of the Convention in the following respects:

(a) the authorisation procedure does not appear capable of ensuring that retained communications data is accessed by the authorities solely when that is "necessary in a democratic society" (see paragraphs 400 to 406 above);

(b) no clear time-limits have been laid down for destroying data accessed by the authorities in the course of criminal proceedings (see paragraph 408 above);

(c) no publicly available rules exist on the storing, accessing, examining, using, communicating and destroying communications data accessed by the authorities (see paragraph 409 above);

(d) the oversight system, as currently organised, does not appear capable of effectively checking abuse (see paragraphs 410 to 415 above);

(e) the notification arrangements, as currently operating, are too narrow (see paragraphs 416 and 417 above); and

(f) it does not appear that there is an effective remedy (see paragraphs 379 to 381 and 418 above).

420. It follows that those laws do not fully meet the "quality of law" requirement and are incapable of keeping the "interference" entailed by the system of retention and accessing of communications data in Bulgaria to what is "necessary in a democratic society".

421. There has therefore been a breach of Article 8 of the Convention in this respect as well.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

422. 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

1. The applicants' claims and the Government's comments on them

423. The first and second applicants claimed 5,000 euros (EUR) each in respect of the alleged frustration and disappointment flowing from the defects marring the secret surveillance system in Bulgaria, which had been illustrated by many scandals revealing cases of unlawful and abusive surveillance.

424. The third and fourth applicants claimed an unspecified sum in respect of the non-pecuniary damage allegedly suffered by them owing to the breach of their privacy rights resulting from the incompatibility of the laws governing secret surveillance and the retention and accessing of communications data with the requirements of the Convention.

425. The Government contested the claims in full, noting that in previous such cases nothing had been awarded in respect of non-pecuniary damage.

2. The Court's assessment

426. The findings of violation amount to sufficient just satisfaction for any non-pecuniary damage suffered by the applicants as a result of the two breaches of Article 8 of the Convention found in this case (see *Roman Zakharov*, § 312, and *Centrum för rättvisa*, §§ 379-80, both cited above).

427. That said, under Article 46 a judgment in which the Court finds a violation of the Convention or its Protocols imposes on the respondent State an obligation to choose, subject to supervision by the Committee of Ministers, the general and/or, if appropriate, individual measures to be taken in its domestic legal order to end the violation and make all feasible reparation for its consequences in a way to restore as far as possible the situation which would have obtained if it had not taken place. Moreover, it follows from the Convention, and from Article 1 in particular, that in ratifying it the Contracting States undertook to ensure that their domestic laws would be compatible with it (see *Roman Zakharov*, cited above, § 311).

428. In this case, as far as secret surveillance is concerned, these general measures will have to supplement those which the Bulgarian authorities have already taken to execute *Association for European Integration and Human Rights and Ekimdzhiev* (cited above).

B. Costs and expenses

1. The applicants' claims and the Government's comments on them

429. The first and second applicants did not seek reimbursement of any lawyers' fees, saying that their representatives had worked on the case for free. They did, however, jointly seek reimbursement of BGN 1,032 incurred for the translation of their submissions into English, and BGN 25.50 in postage. They requested that any award in that respect be made payable to Ekimdzhiev and Partners, the law firm in which their representatives worked. In support of their claims, they submitted two contracts for translation services and postal receipts.

430. The third and fourth applicants sought reimbursement of EUR 2,750 in lawyers' fees incurred for their representation before the Court by, respectively, Mr A.A. Kashamov (EUR 750) and Mr A.E. Kashamov (EUR 2,000). In support of those claims, they submitted contracts for legal services between, respectively, the Access to Information Foundation and Mr A.E. Kashamov and between Mr A.E. Kashamov and Mr A.A. Kashamov, time-sheets and receipts.

431. The Government contested the quantum of the first and second applicants' claim for translation expenses, and the third and fourth

applicants' claim for lawyers' fees. In their view, those were both exorbitant.

2. The Court's assessment

432. According to the Court's case-law, applicants are entitled to the reimbursement of their costs and expenses, but only to the extent that these were actually and necessarily incurred and are reasonable as to quantum.

433. In this case, there is no reason to suspect that the translations costs and postage claimed by the first and second applicants (see paragraph 429 above) have not been actually incurred by them. In view of the volume of those applicants' submissions, the translation costs can also be seen as necessary and reasonable as to quantum. They must hence be awarded in full. Converted into euros, those sums come respectively to EUR 527.65 and EUR 13.04, which gives EUR 540.69 in total. To them should be added any tax that may be chargeable to those applicants. As requested by them, the sums are to be paid into the bank account of Ekimdzhiev and Partners, the law firm in which their representatives work.

434. In view of the complexity of the issues raised by the case, the legal fees claimed by the third and fourth applicants (see paragraph 430 above) can likewise be accepted as necessary and reasonable as to quantum. They must therefore be awarded in full, net of any tax that may be chargeable to those applicants.

C. Default interest

435. 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, UNANIMOUSLY,

1. *Joins* the Government's objections regarding the applicants' victim status and the exhaustion of domestic remedies in relation to the complaint concerning the system of secret surveillance to the merits, and *rejects* them;

2. *Joins* the Government's objections regarding the applicants' victim status and the exhaustion of domestic remedies in relation to the complaint concerning the retention and subsequent accessing of communications data to the merits, and *rejects* them;

3. *Declares* the application admissible;

4. *Holds* that there has been a violation of Article 8 of the Convention with respect to the system of secret surveillance in Bulgaria;

5. *Holds* that there has been a violation of Article 8 of the Convention with respect to the system of retention and subsequent accessing of communications data in Bulgaria;

6. *Holds* that the findings of violation constitute in themselves sufficient just satisfaction for any non-pecuniary damage suffered by the four applicants on account of the two breaches of Article 8 of the Convention found in the case;

7. *Holds*
   (a) that the respondent State is to pay the applicants, within three months from the date on which this judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts in respect of costs and expenses, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
      (i) jointly to the first and second applicants, EUR 540.69 (five hundred forty euros and sixty-nine cents), plus any tax that may be chargeable to them, to be paid into the bank account of Ekimdzhiev and Partners, the law firm in which those applicants' representatives work;
      (ii) to the third applicant, EUR 750 (seven hundred fifty euros), plus any tax that may be chargeable to him;
      (iii) to the fourth applicant, EUR 2,000 (two thousand euros), plus any tax that may be chargeable to it;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

8. *Dismisses* the remainder of the applicants' claims for just satisfaction.

Done in English, and notified in writing on 11 January 2022, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Andrea Tamietti	Tim Eicke
Registrar	President