CONSEIL DE L'EUROPE

COUNCIL OF EUROPE

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

THIRD SECTION

DECISION

AS TO THE ADMISSIBILITY OF

Application no. 54934/00
by Gabriele WEBER and Cesar Richard SARAVIA
against Germany

The European Court of Human Rights (Third Section), sitting on 29 June 2006 as a Chamber composed of:

Mr B.M. ZUPANČIČ, *President*,
Mr L. CAFLISCH,
Mr C. BÎRSAN,
Mr V. ZAGREBELSKY,
Mr E. MYJER,
Mr DAVID THÓR BJÖRGVINSSON, *judges*,
Mr A. ZIMMERMANN, ad hoc *judge*,
and Mr V. BERGER, *Section Registrar*,

Having regard to the above application lodged on 10 January 2000,

Having regard to the observations submitted by the respondent Government and the observations in reply submitted by the applicants,

Having deliberated, decides as follows:

THE FACTS

1. The first applicant, Ms Gabriele Weber, is a German national. The second applicant, Mr Cesar Richard Saravia, is a Uruguayan national. Both applicants live in Montevideo (Uruguay). They were represented before the Court by Mr W. Kaleck, a lawyer practising in Berlin, and by Mr E. Schwan, a university professor in Berlin. The German Government ("the Government") were represented by their Agents, Mr K. Stoltenberg,

Ministerialdirigent, and, subsequently, Mrs A. Wittling-Vogel, *Ministerialdirigentin*, of the Federal Ministry of Justice.

A. The circumstances of the case

2. The facts of the case, as submitted by the parties, may be summarised as follows.

3. The case concerns several provisions of the Act of 13 August 1968 on Restrictions on the Secrecy of Mail, Post and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*), also called "the G 10 Act", as modified by the Fight against Crime Act of 28 October 1994 (*Verbrechensbekämpfungsgesetz*).

4. It notably concerns the extension of the powers of the Federal Intelligence Service (*Bundesnachrichtendienst*) with regard to the recording of telecommunications in the course of so-called strategic monitoring, as well as the use (*Verwertung*) of personal data obtained thereby and their transmission to other authorities. Strategic monitoring is aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences (see in detail "Relevant domestic law and practice" below, paragraphs 18 *et seq.*). In contrast, so-called individual monitoring, that is, the interception of telecommunications of specific persons, serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed.

5. The first applicant is a freelance journalist who works for various German and foreign newspapers, radio and television stations on a regular basis. In particular, she investigates matters that are subject to the surveillance of the Federal Intelligence Service, notably armaments, preparations for war, drug and arms trafficking and money laundering. In order to carry out her investigations, she regularly travels to different countries in Europe and South and Central America, where she also meets the persons she wants to interview.

6. The second applicant, an employee of Montevideo City Council, submitted that he took messages for the first applicant when she was on assignments, both from her telephone and from his own telephone. He then transmitted these messages to wherever she was.

7. On 19 November 1995 the applicants lodged a constitutional complaint with the Federal Constitutional Court.

8. They alleged that certain provisions of the Fight against Crime Act amending the G 10 Act disregarded their fundamental rights, notably the right to secrecy of telecommunications (Article 10 of the Basic Law), the right to self-determination in the sphere of information (Article 2 § 1 and Article 1 § 1 of the Basic Law), freedom of the press (Article 5 § 1 of the

Basic Law) and the right to effective recourse to the courts (Article 19 § 4 of the Basic Law).

9. In the applicants' submission, technological progress made it possible to intercept telecommunications everywhere in the world and to collect personal data. Numerous telecommunications could be monitored, in the absence of any concrete suspicions, with the aid of catchwords which remained secret. Strategic monitoring could then be used in respect of individuals, preventing the press from carrying out effective investigations into sensitive areas covered by the Act.

10. The Federal Constitutional Court, having held a hearing, delivered its judgment on 14 July 1999 (running to 125 pages). It found that the constitutional complaint lodged by the second applicant was inadmissible. The court noted that a constitutional complaint could be lodged directly against a statute if the person concerned could not know whether there had actually been an implementing measure applying the statute to him or her. The complainant, however, had to substantiate sufficiently his or her argument that his or her fundamental rights were likely to be breached by measures taken on the basis of the impugned statute.

11. The Federal Constitutional Court noted that it was irrelevant that the applicants did not reside in Germany, because the impugned provisions were aimed at monitoring international telecommunications. However, it held that, unlike the first applicant, the second applicant had failed to substantiate sufficiently his claim that his rights under the Basic Law were likely to be interfered with by measures based on the impugned provisions of the amended G 10 Act. In the absence of any further details, the mere fact that he dealt with the first applicant's telecommunications in her absence was not sufficient to demonstrate this.

12. Partly allowing the first applicant's constitutional complaint, the Federal Constitutional Court held that certain provisions of the Fight against Crime Act were incompatible or only partly compatible with the principles laid down in the Basic Law (see in detail "Relevant domestic law and practice" below, paragraphs 18 *et seq.*). In particular section 3(1), first and second sentence, point 5, section 3(3), (4), (5), first sentence, (7), first sentence, (8), second sentence, and section 9(2), third sentence of the Act were found to be incompatible with Article 10, Article 5 or Article 19 § 4 of the Basic Law (see paragraphs 26 *et seq.*). It fixed a deadline until 30 June 2001 for the legislature to bring the situation into line with the Constitution.

13. On 29 June 2001 a new version of the G 10 Act entered into force (BGBl. I 2001, pp. 1254, 2298) and the G 10 Act in its version as amended by the Fight against Crime Act of 28 October 1994 ceased to apply.

B. Relevant domestic law and practice

1. The Basic Law

14. The Basic Law provides for the following fundamental rights, in so far as relevant:

Article 5

Right to freedom of expression

"(1) Everyone shall have the right freely to express and disseminate his opinions in speech, writing and pictures and freely to obtain information from generally accessible sources. Freedom of the press and freedom of reporting on the radio and in films shall be guaranteed. There shall be no censorship.

(2) These rights shall be subject to the limitations laid down by the provisions of the general laws and by statutory provisions aimed at protecting young people and to the obligation to respect personal honour."

Article 10

Secrecy of mail, post and telecommunications

"(1) Secrecy of mail, post and telecommunications shall be inviolable.

(2) Restrictions may be ordered only pursuant to a statute. Where such restrictions are intended to protect the free democratic constitutional order or the existence or security of the Federation or of a *Land*, the statute may provide that the person concerned shall not be notified of the restriction and that review by the courts shall be replaced by a system of scrutiny by agencies and auxiliary agencies appointed by the people's elected representatives."

Article 19

Restriction on basic rights

"(4) If a person's rights are violated by a public authority he may have recourse to the courts. If no other jurisdiction has been established, the civil courts shall have jurisdiction. Article 10 § 2, second sentence, remains unaffected by this paragraph."

15. The separation of legislative powers between the Federation and the *Länder* is laid down in Articles 70 et seq. of the Basic Law. Pursuant to Article 70 § 1 the *Länder*, in principle, have the right to legislate in so far as the Basic Law does not confer legislative power on the Federation. Such legislative power is conferred on the Federation, in particular, in Article 73:

"The Federation shall have exclusive power to legislate (*ausschließliche Gesetzgebungskompetenz*) on:

1. foreign affairs and defence, including the protection of civilians;

..."

2. The Act of 13 August 1968 on Restrictions on the Secrecy of Mail, Post and Telecommunications

16. Being the statute envisaged by Article 10 § 2, second sentence, of the Basic Law (cited above, paragraph 14), which provides for exceptions to the general rule of inviolability of telecommunications, the Act of 13 August 1968 on Restrictions on the Secrecy of Mail, Post and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*), also called "the G 10 Act", lays down the conditions under which the authorities may introduce the restrictions referred to in that provision of the Basic Law.

17. In a judgment delivered on 6 September 1978 (*Klass and Others v. Germany*, Series A no. 28) the Court held that the provisions of the G 10 Act of 13 August 1968, in its original version and as regards the monitoring of individuals, did not contravene the Convention. It found that the German legislature was justified in considering that the interference resulting from the legislation in question with the rights guaranteed by Article 8 § 1 of the Convention was necessary in a democratic society within the meaning of paragraph 2 of that Article. The Court also considered that the remedies provided for in the G 10 Act complied with the requirements of Article 13 of the Convention.

3. The Fight against Crime Act of 28 October 1994 in the light of the Federal Constitutional Court's judgment of 14 July 1999

(a) Legislative background

18. The Federal Act of 28 October 1994 on the Fight against Crime amended the G 10 Act. Among other things, it extended the range of subjects in respect of which "strategic monitoring" (as opposed to monitoring of individuals) could be carried out. In the original version of the G 10 Act such monitoring was permitted only in order to detect and avert the danger of an armed attack on the Federal Republic of Germany and at that time was therefore merely focused on the States belonging to the Warsaw Pact. Furthermore, owing to technical progress it had become possible to identify the telephone connections (*Anschlüsse*) involved in an intercepted telecommunication.

19. Pursuant to the provisions of the G 10 Act, which either remained unchanged by the Fight against Crime Act or were not contested in the present case, the Offices for the Protection of the Constitution of both the Federation and the *Länder* (*Verfassungsschutzbehörden des Bundes und der Länder*), the Military Counter-Intelligence Service (*Militärischer Abschirmdienst*) and the Federal Intelligence Service were entitled to monitor and record telecommunications within their own sphere of activities (section 1(1) of the G 10 Act). Monitoring of individuals was limited to serious threats to national security (for example, high treason or threatening

the democratic order) and was permissible only if less intrusive means of investigation had no prospect of success or were considerably more difficult (section 2 of the G 10 Act). As to strategic monitoring, only the head of the Federal Intelligence Service or his deputy were entitled to lodge an application for a surveillance order. The application had to be lodged in writing, had to describe and give reasons for the nature, scope and duration of the measure and had to explain that other means of carrying out the investigations either had no prospect of success or were considerably more difficult (section 4 of the G 10 Act).

20. Restrictions on the secrecy of telecommunications were to be ordered by the Federal Minister assigned by the Chancellor or the highest authority of the *Länder* (in respect of applications by their Offices for the Protection of the Constitution). The order was made in writing and specified the exact nature, scope and duration of the monitoring measure. The duration of the measure was to be limited to a maximum of three months; the execution of the measure could be prolonged for a maximum of three months at a time as long as the statutory conditions for the order were met (see section 5 of the G 10 Act).

21. The monitoring measures authorised were to be carried out under the responsibility of the requesting authority and under the supervision of a staff member qualified to hold judicial office. Monitoring had to be discontinued immediately if the conditions of the monitoring order were no longer met or the measure was no longer necessary (section 7 of the G 10 Act).

22. Section 3(4) provided that the Federal Intelligence Service was to verify whether the personal data obtained by measures taken under subsection 1 of section 3 were necessary to pursue the aims laid down in that subsection.

23. The Federal Constitutional Court found that in its present version, section 3(4) was incompatible with Article 10 and Article 5 § 1, second sentence, of the Basic Law. It found that the provision did not contain sufficient safeguards to guarantee that personal data which were not destroyed or deleted as being unnecessary for the purposes of the Federal Intelligence Service would be used only for the purposes which had justified their collection. Furthermore, the provision also failed to comply with the identification requirements flowing from Article 10. In addition, there were insufficient safeguards to guarantee that the Federal Intelligence Service would only use such data as were relevant for the dangers listed in section 3(1). Such safeguards should also ensure that the Federal Intelligence Service would take into account the important concerns of non-disclosure of sources and confidentiality of editorial work as protected by the freedom of the press under Article 5 § 1 of the Basic Law. The court ruled that, pending the entry into force of legislation in compliance with the Constitution, section 3(4) was to be applied only if the data were specially

marked and were not used for purposes other than those listed in section 3(1).

24. Monitoring measures were supervised by two bodies, the Parliamentary Supervisory Board and the so-called G 10 Commission (see section 9 of the G 10 Act). At the relevant time, the Parliamentary Supervisory Board consisted of nine members of parliament, including representatives of the opposition. The Federal Minister authorising monitoring measures had to inform the board at least every six months about the implementation of the G 10 Act (section 9(1) of the G 10 Act).

25. The G 10 Commission consisted of a president who was qualified to hold judicial office and three additional members who were appointed by the Parliamentary Supervisory Board for the duration of one legislative term and who were independent in the exercise of their functions (see section 9(4) of the G 10 Act). The Federal Minister authorising surveillance measures had to inform the G 10 Commission monthly about planned monitoring measures and had to obtain its consent (section 9(2) of the G 10 Act; see in detail below, paragraphs 55-58). Moreover, the Federal Minister had to inform the Commission whether or not persons concerned by such measures had been notified of them. If the Commission decided that notification was necessary, the Federal Minister had to arrange for it to be given without undue delay (section 9(3) of the G 10 Act).

(b) Section 3(1) of the amended G 10 Act: Dangers for the avoidance of which monitoring of telecommunications could be ordered

26. Section 1(1), points 1 and 2, in conjunction with section 3(1), first and second sentence, authorised the monitoring of wireless telecommunications, that is, telecommunications which were not effected via fixed telephone lines, but, for example, via satellite connections (*Überwachung nicht leitungsgebundener Fernmeldeverkehrsbeziehungen*).

27. Section 3(1), first sentence, provided that restrictions on the secrecy of telecommunications could be ordered by the competent Federal Minister with the approval of the Parliamentary Supervisory Board, on an application by the Federal Intelligence Service, for international wireless telecommunications. Under the second sentence of that provision, such restrictions were permitted only in order to collect information about which knowledge was necessary for the timely identification and avoidance of certain dangers, namely

1. an armed attack on the Federal Republic of Germany;

2. the commission of international terrorist attacks in the Federal Republic of Germany;

3. international arms trafficking within the meaning of the Control of Weapons of War Act and prohibited external trade in goods, data-processing programmes and technologies in cases of considerable importance;

4. the illegal importation of drugs in substantial quantities into the territory of the Federal Republic of Germany;

5. the counterfeiting of money (*Geldfälschung*) committed abroad;

6. the laundering of money in the context of the acts listed under points 3 to 5. Pursuant to section 3(1), third sentence, restrictions on the secrecy of telecommunications could also be ordered for telecommunications via fixed telephone lines and for mail in order to identify and avert the dangers listed in section 3(1), second sentence, point 1.

28. The Federal Constitutional Court found that, pursuant to Article 73, point 1, of the Basic Law (see paragraph 15 above), the federal legislature had exclusive legislative power to regulate the matters listed in section 3(1) of the amended G 10 Act, as they concerned foreign affairs.

29. However, the Federal Constitutional Court took the view that allowing the monitoring of telecommunications in order to prevent the counterfeiting of money abroad, in accordance with point 5 of section 3(1) in its present wording, constituted a disproportionate interference with the secrecy of telecommunications as protected by Article 10 of the Basic Law. It argued that this danger as such could not be considered to be as serious as an armed attack on the German State or any of the other dangers listed in section 3(1). The counterfeiting of money should therefore be included in section 3(1) only if it was restricted to cases in which it threatened the monetary stability of the Federal Republic of Germany. The court ruled that, pending the entry into force of legislation in compliance with the Constitution, section 3(1), second sentence, point 5, was to be applied only if the counterfeiting of money abroad threatened monetary stability in Germany.

30. In practice, wireless telecommunications (as opposed to telecommunications via fixed telephone lines) comprised some ten per cent of the total volume of telecommunications at the relevant time. However, given technical progress, the volume of such telecommunications was expected to rise in the future.

31. Technically, telecommunications via satellite links (with the satellites being positioned some 36,000 km above the equator) could be intercepted from sites in Germany if the signal reflected by the satellite (the "downlink") covered the area in which the station was located. The area covered by the satellite beam depended on the satellite technology used. Whereas signals downlinked by older satellites often "beamed" across one-third of the earth's surface, more modern satellites could concentrate their downlink on smaller areas. Signals could be intercepted everywhere within the area covered by the beam. International radio relay links (*Richtfunkstrecken*) could be intercepted from interception sites on German soil only if the radio relay transmission was effected within close proximity of these sites.

(c) Section 3(2) of the amended G 10 Act: Monitoring through catchwords

32. Pursuant to section 3(2), the Federal Intelligence Service was only authorised to carry out monitoring measures with the aid of catchwords (*Suchbegriffe*) which served, and were suitable for, the investigation of the dangers described in the monitoring order (first sentence). The second sentence of that provision prohibited the catchwords from containing distinguishing features (*Identifizierungsmerkmale*) allowing the interception of specific telecommunications. However, this rule did not apply to telephone connections situated abroad if it could be ruled out that connections concerning German nationals or German companies were deliberately being monitored (third sentence). The catchwords had to be listed in the monitoring order (fourth sentence). The execution of the monitoring process as such had to be recorded in minutes by technical means and was subject to supervision by the G 10 Commission (fifth sentence). The data contained in these minutes could be used only for the purposes of reviewing data protection and had to be deleted at the end of the year following their recording (sixth and seventh sentences).

d. Section 3(3) of the amended G 10 Act: Restrictions on the permitted use of personal data

33. Section 3(3), first sentence, provided that personal data (*personenbezogene Daten*) obtained through the interception of telecommunications could only serve the prevention, investigation and prosecution of offences listed in section 2 of the Act and in certain other provisions, notably of the Criminal Code. These offences included, in particular, high treason against the peace or security of the State, crimes threatening the democratic order, the external security of the State or the security of the allied forces based in the Federal Republic of Germany, the formation of terrorist associations, murder, manslaughter, robbery, the forgery of payment cards or cheques, fraud relating to economic subsidies, infiltration of foreigners and the production, importation and trafficking of illegal drugs. Personal data thus obtained could be used only if the person concerned was either subject to individual monitoring under section 2 of the Act or if there were factual indications (*tatsächliche Anhaltspunkte*) for suspecting a person of planning, committing or having committed one of the offences mentioned above. This catalogue of offences for the investigation of which knowledge obtained by strategic monitoring could be used was considerably enlarged by the amendment of the G 10 Act at issue.

34. Pursuant to section 3(3), second sentence, the obligation on the Federal Intelligence Service to inform the Federal Government of its findings obtained by strategic monitoring, including personal data, under section 12 of the Act on the Federal Intelligence Service remained unaffected.

35. The Federal Constitutional Court found that section 3(3), second sentence, in its present version, failed to comply with Article 10 and Article 5 § 1, second sentence, of the Basic Law. The provision did not contain sufficient safeguards to guarantee that the duty of the Federal Intelligence Service to report to the Federal Government, which included the transmission of personal data, would be performed solely for the purposes which had justified the collection of the data (*Zweckbindung*). Furthermore, the provision failed to comply with the identification requirements (*Kennzeichnungspflicht*) flowing from Article 10. Ensuring that personal data were not used for illegal purposes was possible only if it remained discernible that the data concerned had been obtained by means of an interference with the secrecy of telecommunications. Likewise, there were no safeguards ensuring that the Federal Government did not keep or use the personal data transmitted to them for purposes other than those listed in section 3(1). The court ruled that, pending the entry into force of legislation in compliance with the Constitution, section 3(3), second sentence, was to be applied only if the personal data contained in the report to the Federal Government were marked and remained bound up with the purposes which had justified their collection.

(e) Section 3(5) of the amended G 10 Act: Transmission of data to other authorities

36. Section 3(5), first sentence, provided that the data obtained in the circumstances described in subsection 1 of section 3 had to be transmitted to the Offices for the Protection of the Constitution of the Federation and of the *Länder*, to the Military Counter-Intelligence Service, to the Customs Investigation Office (*Zollkriminalamt*), to the public prosecutor's offices and to certain police services for the purposes laid down in subsection 3 of section 3 in so far as this was necessary for the recipient authorities to carry out their duties.

37. Pursuant to section 3(5), second sentence, the decision to transmit data was to be taken by a staff member who was qualified to hold judicial office.

38. The Federal Constitutional Court found that the federal legislature's exclusive legislative power under Article 73, point 1, of the Basic Law (see paragraph 15 above) to regulate matters concerning foreign affairs also covered the transmission to other authorities of information obtained by the Federal Intelligence Service in the performance of its tasks as provided for in section 3(5) of the amended G 10 Act. The federal legislature merely had to provide guarantees that the further use of the data did not disregard the primary function of the monitoring measures.

39. The Federal Constitutional Court further found that section 3(5) was not fully compatible with Article 10 and Article 5 § 1, second sentence, of the Basic Law. It held that Article 10 did not prohibit the transmission to the

authorities listed in section 3(5), first sentence, of information which was relevant for the prevention and investigation of criminal offences. This finding was not called into question by the fact that the initial collection of data by means of the random interception of telecommunications in order to prevent or investigate offences, without any prior suspicion of a specific offence being planned or having been committed, would breach Article 10.

40. However, in the opinion of the Federal Constitutional Court, the transmission of data under section 3(5), first sentence, in its present version, disproportionately interfered with the right to secrecy of telecommunications and freedom of the press. The transmission of data constituted a further serious interference with the secrecy of telecommunications, because criminal investigations could be instituted against persons concerned by the interception of telecommunications which had been carried out without any prior suspicion of an offence. Consequently, such transmission was proportionate only if it served the protection of an important legal interest and if there was a sufficient factual basis for the suspicion that criminal offences were being planned or had been committed.

41. Section 3(5), first sentence, read in conjunction with section 3(3), did not fully comply with these requirements.

42. The catalogue of offences in respect of which the transmission of data was permitted also included less serious offences such as fraud relating to economic subsidies. Moreover, the impugned provision authorised the transmission of data in cases in which there were merely factual indications for the suspicion that one of the offences listed in that provision had been committed or was even only being planned. The transmission of data for the investigation of an offence which had already been committed should be authorised only if the factual basis for the transmission was the same as that required by section 100a of the Code of Criminal Procedure. Section 100a provided, however, that interferences with the secrecy of telecommunications in order to investigate crimes required the presence of specific facts – as opposed to mere factual indications – warranting the suspicion that the person concerned had committed an offence listed in that provision. As regards the transmission of data for the prevention of crime, the combination of the elements that mere factual indications were sufficient, that the mere planning of an offence could suffice and that transmission could also be justified in the case of less serious offences led to a disproportionate interference with the fundamental rights affected.

43. The Federal Constitutional Court further found that section 3(5), second sentence, was likewise not compatible with the right to secrecy of telecommunications. It considered it unnecessary to entrust the decision on transmission of data to an independent body. However, there was no requirement to record in minutes the transmission or the destruction or

deletion of the data. This rendered effective supervision of the transmission of the data impossible.

44. The Federal Constitutional Court ruled that, pending the entry into force of legislation in compliance with the Constitution, section 3(5), first sentence, could be applied provided that data were only transmitted if specific facts aroused the suspicion that offences listed in section 3(3) had been committed. Furthermore, the transmission had to be recorded in minutes.

(f) Section 3(6) and (7) and section 7(4) of the amended G 10 Act: Destruction of data

45. Section 3(6) and (7) and section 7(4) regulated the procedure for destruction of the data obtained by strategic monitoring.

46. Section 3(6) provided that if the data obtained in the circumstances set out in section 3(1) were no longer necessary to achieve the purposes listed in that provision and if they did not have to be transmitted to other authorities pursuant to section 3(5), they had to be destroyed and deleted from the files under the supervision of a staff member who was qualified to hold judicial office (first sentence). The destruction and deletion had to be recorded in minutes (second sentence). It was necessary to verify every six months whether the conditions for destruction or deletion were met (third sentence).

47. Section 3(7) provided that the recipient authorities likewise were to verify whether they needed the data transmitted to them in order to achieve the aims laid down in section 3(3) (first sentence). If this was not the case, they also had to destroy the data immediately (second sentence). The destruction could be dispensed with if separation of the data from other information which was necessary for the fulfilment of the tasks set was impossible or could only be carried out through unjustifiable effort; the use of such data was prohibited (third sentence).

48. Section 7(4), first sentence, provided that personal data obtained by means of monitoring measures pursuant to sections 2 and 3 about a person involved in the telecommunications monitored had to be destroyed if they were no longer necessary for the purposes listed in the Act and could no longer be of significance for an examination by the courts of the legality of the measure. The destruction had to be carried out under the supervision of a person qualified to hold judicial office. Pursuant to section 7(4), second sentence, the destruction had to be recorded in minutes. It was necessary to examine every six months whether personal data obtained could be destroyed (third sentence). Access to data which were merely kept for the purpose of judicial review of the monitoring measure had to be blocked (fourth sentence). They could only be used for that purpose (fifth sentence).

49. The Federal Constitutional Court found that the provisions on the destruction of data laid down in section 3(6) and (7), second and third

sentences, and section 7(4) complied with Article 19 § 4 of the Basic Law. The provisions, however, had to be interpreted so as not to frustrate judicial review of monitoring measures. This meant that data could only be destroyed six months after the person concerned had been notified that monitoring measures had been taken.

50. However, the Federal Constitutional Court considered section 3(7) to be incompatible with Article 10 of the Basic Law. It was necessary for the recipient authorities to mark the data as having been obtained by means of the interception of telecommunications. Otherwise, following verification that the information obtained was relevant for the tasks of the authorities concerned, personal data could be saved in a manner which made it impossible to identify them as resulting from the strategic monitoring of telecommunications. The restrictions on the permitted use of these data pursuant to section 3(3) would thereby be undermined. The court ruled that, pending the entry into force of legislation in compliance with the Constitution, section 3(7) could be applied provided that the data were marked as described.

(g) Section 3(8) of the amended G 10 Act: Notification of the persons concerned by the monitoring

51. Section 3(8), first sentence, provided that the Federal Intelligence Service or the recipient authorities had to inform the persons monitored about the restriction imposed on the secrecy of telecommunications as soon as such notification could occur without jeopardising the achievement of the aim pursued by the restriction and the use of the data. Pursuant to section 3(8), second sentence, no notification was given if the data obtained had been destroyed within three months after their receipt by the Federal Intelligence Service or the recipient authorities.

52. The Federal Constitutional Court considered the restriction on the duty of notification as such, as laid down in section 3(8), first sentence, to be compatible with the Basic Law. By virtue of Article 10 § 2, first and second sentences, taken in conjunction with Article 19 § 4, third sentence, of the Basic Law, no notification had to be given if this served to protect the German State or its democratic order or if disclosure of the information obtained or the methods used to this end threatened the fulfilment of the tasks of the authorities concerned.

53. However, section 3(8), second sentence, violated Article 10 and Article 19 § 4 of the Basic Law. There were no safeguards precluding the data from being used before their destruction within the three-month period. The mere destruction of the data within that period alone did not, however, justify dispensing with the duty of notification irrespective of the prior use of the data.

54. The court ruled that, pending the entry into force of legislation in compliance with the Constitution, section 3(8) could be applied provided that the data had not been used before their destruction.

(h) Section 9(2) of the G 10 Act: Supervision of monitoring measures

55. Section 9(2) provided for supervision of the monitoring measures by an independent body, the so-called G 10 Commission.

56. Pursuant to section 9(2), first sentence, the competent Federal Minister was to inform the G 10 Commission on a monthly basis about the measures he had ordered to restrict the secrecy of telecommunications before such measures were implemented.

57. The Federal Minister could, however, order the execution of the measure before having informed the G 10 Commission if there was a risk that a delay might frustrate the purpose of the measure (second sentence of section 9(2)). The Commission gave a decision of its own motion or further to complaints contesting the legality and necessity of monitoring measures (third sentence). Monitoring orders which the Commission deemed illegal or unnecessary had to be immediately revoked by the Minister (fourth sentence).

58. The Federal Constitutional Court considered that section 9(2), in its present wording, was incompatible with Article 10 of the Basic Law. It failed to provide in a sufficiently clear manner that supervision by the G 10 Commission covered the whole process of obtaining and using the data (including measures taken under section 3(3), (5), (6) and (8)), and not only the monitoring orders by the competent Minister. The court ruled that, pending the entry into force of legislation in compliance with the Constitution, the provision in question was only to be applied if the Commission's supervisory powers extended to measures taken under section 3(3), (5), (6) and (8).

(i) Section 9(6) of the amended G 10 Act: Exclusion of judicial review

59. Section 9(6) excluded the possibility of judicial review in the case of monitoring measures ordered and executed to prevent an armed attack on the territory of the Federal Republic of Germany within the meaning of section 3(1), second sentence, point 1.

60. Pursuant to section 5(5) of the G 10 Act, which remained unchanged in substance, the person concerned had to be notified of measures restricting the secrecy of telecommunications as soon as these measures were discontinued, provided that such notification did not jeopardise the purpose of the restriction (first and second sentence). After notification the person concerned could have recourse to the courts; section 9(6) did not apply (third sentence).

61. The Federal Constitutional Court found that section 9(6) constituted a justified restriction on the secrecy of telecommunications in accordance

with Article 10 § 2, second sentence, of the Basic Law. Moreover, a person concerned by a monitoring measure could have recourse to the courts following notification of the restriction under section 5(5), third sentence, of the G 10 Act. The same applied if the person concerned had learned of the monitoring measure by another means, without having been notified.

4. The new G 10 Act

62. A new version of the G 10 Act, which takes into account the principles laid down by the Federal Constitutional Court in its judgment dated 14 July 1999, entered into force on 26 June 2001.

COMPLAINTS

63. The applicants claimed that certain provisions of the Fight against Crime Act amending the G 10 Act, in their versions as interpreted and modified by the Federal Constitutional Court in its judgment of 14 July 1999, violated their right to respect for their private life and their correspondence as protected by Article 8 of the Convention. They complained in particular about section 3(1), (3), (5), (6), (7) and (8) of the amended G 10 Act.

64. The first applicant further argued that the same provisions of the Fight against Crime Act infringed freedom of the press as guaranteed by Article 10 of the Convention.

65. The applicants also submitted that the destruction of data (section 3(6) and (7), read in conjunction with section 7(4)), the failure to give notice of restrictions on the secrecy of telecommunications (section 3(8)) and the exclusion of judicial review in certain cases (section 9(6)) in accordance with the Act breached Article 13 of the Convention.

THE LAW

A. The Government's objections

1. The submissions of the parties

(a) The Government

66. The Government argued, firstly, that the application was incompatible *ratione personae* with the provisions of the Convention. Both applicants resided in Uruguay and claimed that their Convention rights

had been infringed as regards telecommunications from their telephone connections in that country. The monitoring of telecommunications made from abroad, however, had to be qualified as an extraterritorial act. In accordance with the Court's decision in the case of *Banković and Others v. Belgium and Others* ([GC], no. 52207/99, ECHR 2001-XII), the applicants therefore did not come within Germany's jurisdiction within the meaning of Article 1 of the Convention – a concept which was primarily territorial – on account of that act.

67. Secondly, in the Government's submission, the second applicant had failed to exhaust domestic remedies as required by Article 35 § 1 of the Convention. He had not sufficiently substantiated in his constitutional complaint his argument that his rights under the Basic Law were likely to be interfered with by measures taken on the basis of the impugned provisions of the amended G 10 Act. The Federal Constitutional Court had therefore dismissed his complaint as being inadmissible. Moreover, the first applicant had failed to exhaust domestic remedies in so far as she had complained that section 3(2), third sentence, of the amended G 10 Act violated her Convention rights. She had failed to show in her complaint to the Federal Constitutional Court that she was affected by the provision in question and to what extent.

68. Thirdly, in the Government's view, the applicants could not claim to be victims of a violation of their Convention rights. They referred to their reasoning with regard to exhaustion of domestic remedies in that connection. Moreover, in so far as the Federal Constitutional Court had already declared the impugned provisions to be unconstitutional, the applicants could no longer claim to be victims of a violation of their Convention rights. In particular, they did not have a legitimate interest in obtaining a decision in so far as that court permitted the continued application of those provisions on a provisional basis.

(b) The applicants

69. The applicants contested those submissions. As to the applications' compatibility *ratione personae* with the Convention, the first applicant argued that she came within German jurisdiction within the meaning of Article 1 of the Convention as she was a German national. Both applicants further argued that it could not be decisive that the impugned acts had taken effect abroad. Otherwise a respondent State could circumvent its obligations under the Convention.

70. The applicants submitted that they had exhausted domestic remedies as they had both obtained a judgment of the Federal Constitutional Court, delivered on 14 July 1999.

71. The applicants further argued that they had not lost their status as victims of violations of their Convention rights in so far as they had not been granted the redress sought in their constitutional complaints. They

stressed that the powers of the Federal Intelligence Service had remained unchanged in the new version of the G 10 Act of 2001 in so far as the Federal Constitutional Court had not objected to them. It was in the nature of secret monitoring that they could not prove that they had actually been subjected to it. However, it was very likely that because of their activities, they had used catchwords within the meaning of section 3(2) of the G 10 Act, which had caused their communications to be recorded and analysed.

2. The Court's assessment

72. The Court does not consider it necessary in the present case to rule on the objections made by the Government since, even assuming that the applications are compatible *ratione personae* with the Convention, that domestic remedies have been exhausted and that both applicants can claim to be victims of Convention violations, it considers that the applications are in any event inadmissible for the reasons set out below.

B. Complaints under Article 8 of the Convention

73. The applicants submitted that certain provisions of the Fight against Crime Act amending the G 10 Act, in their versions as interpreted and modified by the Federal Constitutional Court, violated their right to respect for their private life and their correspondence.

74. In particular, the applicants complained about five measures. Firstly, they complained about the process of strategic monitoring (section 3(1), taken in conjunction with section 1(1), point 2, of the G 10 Act). Secondly, they contested the transmission and use of personal data pursuant to section 3(3), second sentence, of the G 10 Act. Thirdly, they complained about the transmission of personal data to the Offices for the Protection of the Constitution and other authorities and its use by them pursuant to section 3(5) of the G 10 Act. Fourthly, they contested the destruction of personal data under section 3(6) and (7), taken in conjunction with section 7(4), of the G 10 Act. Fifthly, they contested the provision authorising the refusal to give notice of restrictions on the secrecy of telecommunications (section 3(8) of the G 10 Act).

75. The applicants invoked Article 8 of the Convention which, in so far as relevant, reads:

> "1. Everyone has the right to respect for his private ... life, ... and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

1. Whether there was an interference

76. The Government conceded that the impugned provisions of the amended G 10 Act, in so far as they authorised the monitoring of telecommunications and the use of data obtained thereby, interfered with the secrecy of telecommunications as protected by Article 8. The applicants took the same view.

77. The Court reiterates that telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (see, *inter alia*, *Klass and Others*, cited above, p. 21, § 41; *Malone v. the United Kingdom*, judgment of 2 August 1984 Series A no. 82, pp. 30-31, § 64; and *Lambert v. France*, judgment of 24 August 1998, *Reports of Judgments and Decisions* 1998-V, pp. 2238-39, § 21).

78. The Court further notes that the applicants, even though they were members of a group of persons who were likely to be affected by measures of interception, were unable to demonstrate that the impugned measures had actually been applied to them. It reiterates, however, its findings in comparable cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (see *Klass and Others*, cited above, p. 21, § 41, and *Malone*, cited above, pp. 30-31, § 64).

79. Consequently, the impugned provisions of the amended G 10 Act, in so far as they authorise the interception of telecommunications, interfere with the applicants' right to respect for private life and correspondence. Furthermore, the Court, like the Federal Constitutional Court, takes the view that the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8 (see, *mutatis mutandis*, *Leander v. Sweden*, judgment of 26 March 1987, Series A no. 116, p. 22, § 48; *Amann v. Switzerland* [GC], no. 27798/95, § 70, ECHR 2000-II; and *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V). Moreover, the impugned provisions interfere with these rights in so far as they provide for the destruction of the data obtained and for the refusal to notify the persons concerned of surveillance measures taken in that this may serve to conceal monitoring measures interfering with the applicants' rights under Article 8 which have been carried out by the authorities.

2. Whether the interference was justified

80. Such interferences are justified by the terms of paragraph 2 of Article 8 if they are "in accordance with the law", pursue one or more of the legitimate aims referred to in paragraph 2 and, furthermore, are "necessary in a democratic society" in order to achieve them.

(a) Were the interferences "in accordance with the law"?

81. The Government took the view that the interferences were in accordance with the law. On the one hand, they were not contrary to public international law because the monitoring of wireless telecommunications did not interfere with the territorial sovereignty of foreign States. In any event, the first applicant could not rely on an alleged violation of a State's territorial sovereignty in the context of an individual application to the Court. On the other hand, the interferences in question were based on the amended provisions of the G 10 Act and, in so far as the Federal Constitutional Court had declared some of the impugned provisions to be unconstitutional, on that court's rulings concerning the manner in which these provisions were to be applied during a transitional period. In particular, section 3(5), as confirmed by the Federal Constitutional Court, constituted a sufficient legal basis for the transmission of data by the Federal Intelligence Service to other authorities.

82. The Government further submitted that the circumstances in which telecommunications could be monitored and the data thus obtained be used were set out in a precise manner in the amended provisions of the G 10 Act and in the Constitutional Court's judgment. There were, in particular, sufficient procedural safeguards against abuse of powers of surveillance.

83. The applicant argued that the interception of telecommunications interfered illegally with the sovereignty of the foreign States in which the persons being monitored resided. Moreover, section 3(5) of the amended G 10 Act provided no valid legal basis for the transmission of information obtained by means of the interception of telecommunications to the Offices for the Protection of the Constitution of the Federation and of the *Länder* and to the Military Counter-Intelligence Service. Contrary to the Federal Constitutional Court's view, Article 73, point 1, of the Basic Law did not authorise the federal legislature to enact such a regulation.

84. The Court reiterates that the expression "in accordance with the law" within the meaning of Article 8 § 2 requires, firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law (see, among other authorities, *Kruslin v. France*, judgment of 24 April 1990, Series A no. 176-A, p. 20, § 27; *Huvig v. France*, judgment of 24 April 1990, Series A no. 176-B,

p. 52, § 26; *Lambert*, cited above, p. 2239, § 23; and *Perry v. the United Kingdom*, no. 63737/00, § 45, ECHR 2003-IX).

i. Whether there was a statutory basis in German law

85. The Court notes at the outset that in the present case, the interference with the applicants' right to respect for their private life and correspondence resulted from provisions of the amended G 10 Act, an Act passed by Parliament and applicable in the manner set out by the Federal Constitutional Court in its judgment of 14 July 1999.

86. The Court further observes that the applicants considered the impugned provisions of the amended G 10 Act not to constitute a valid statutory basis, in the first place because the interception of telecommunications interfered illegally with the sovereignty of the foreign States in which the persons monitored resided.

87. The Court reiterates that the term "law" within the meaning of the Convention refers back to national law, including rules of public international law applicable in the State concerned (see, *mutatis mutandis*, *Groppera Radio AG and Others v. Switzerland*, judgment of 28 March 1990, Series A no. 173, p. 26, § 68; *Autronic AG v. Switzerland*, judgment of 22 May 1990, Series A no. 178, p. 25, § 56; *Stocké v. Germany*, judgment of 19 March 1991, Series A no. 199, p. 19, § 54; and *Öcalan v. Turkey* [GC], no. 46221/99, § 90, ECHR 2005-IV). As regards allegations that a respondent State has violated international law by breaching the territorial sovereignty of a foreign State, the Court requires proof in the form of concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign State and therefore contrary to international law (see, in particular, *Öcalan*, cited above, § 90).

88. The Court observes that the impugned provisions of the amended G 10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.

89. The Court further observes that the applicants disputed, secondly, that section 3(5) of the amended G 10 Act provided a valid legal basis for the transmission of information. They argued that the federal legislature had not been authorised *vis-à-vis* the *Länder* legislatures, by the relevant provisions on legislative powers laid down in the Basic Law, in particular

Article 73, to adopt such a provision. They were, therefore, claiming in substance that the impugned provision of the amended G 10 Act failed to comply with domestic law of a higher rank, namely the provisions on legislative powers laid down in the German Constitution.

90. The Court reiterates in this connection that, whilst it is true that no interference can be considered to be "in accordance with law" unless the decision – or statutory provision – occasioning it complied with the relevant domestic law – of a higher rank – the logic of the system of safeguards established by the Convention sets limits on the scope of the power of review exercisable by the Court in this respect. It is in the first place for the national authorities, notably the courts, to interpret and apply the domestic law: the national authorities are, in the nature of things, particularly qualified to settle the issues arising in this connection (see, *mutatis mutandis*, *Kruslin*, cited above, p. 21, § 29, and *Barthold v. Germany*, judgment of 25 March 1985, Series A no. 90, pp. 22-23, § 48). In a sphere covered by written law, the "law" is therefore the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments, and the Court cannot question the national courts' interpretation except in the event of flagrant non-observance of, or arbitrariness in the application of, the domestic legislation in question (see, *inter alia*, *Kruslin*, cited above, p. 21, § 29; *Société Colas Est and Others v. France*, no. 37971/97, § 43, ECHR 2002-III; and, *mutatis mutandis*, *Lavents v. Latvia*, no. 58442/00, § 114, 28 November 2002; and *Leyla Şahin v. Turkey* [GC], no. 44774/98, § 88, ECHR 2005-...).

91. The Court notes that the Federal Constitutional Court, in its judgment in the present case, found that the exclusive legislative power vested in the federal legislature in the sphere of foreign affairs pursuant to Article 73, point 1, of the Basic Law also authorised it to legislate in the matters laid down in section 3(5) of the amended G 10 Act. The Court considers that the national courts' interpretation to the effect that the transmission to other authorities of information obtained by the Federal Intelligence Service in the performance of its tasks was covered by the federal legislature's powers in the sphere of foreign affairs does not disclose any flagrant non-observance of the Basic Law or arbitrariness in its application. It is accordingly satisfied that there was a sufficient legal basis for the impugned measure.

ii. Quality of the law

92. The second requirement which emerges from the phrase "in accordance with the law" – the accessibility of the law – does not raise any problem in the instant case.

93. As to the third requirement, the law's foreseeability, the Court reiterates that foreseeability in the special context of secret measures of

surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, *inter alia*, *Leander*, cited above, p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, *inter alia*, *Malone*, cited above, p. 32, § 67; *Huvig*, cited above, pp. 54-55, § 29; and *Rotaru*, cited above, § 55). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, judgment of 25 March 1998, *Reports* 1998-II, pp. 542-43, § 72, and *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, *Reports* 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Malone*, ibid.; *Kopp*, cited above, p. 541, § 64; *Huvig*, cited above, pp. 54-55, § 29; and *Valenzuela Contreras*, ibid.).

94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, pp. 32-33, § 68; *Leander*, cited above, p. 23, § 51; and *Huvig*, cited above, pp. 54-55, § 29).

95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig*, cited above, p. 56, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, pp. 1924-25, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003).

96. Turning to the present case, the Court observes that section 3(1) of the amended G 10 Act, as interpreted by the Federal Constitutional Court, enumerated in its second sentence, points 1-6, the exact offences for the prevention of which the strategic interception of telecommunications could

be ordered. The amended G 10 Act therefore defined in a clear and precise manner the offences which could give rise to an interception order.

97. The Court further observes that the conditions for strategic monitoring, as laid down in section 3(1) and (2) of the amended G 10 Act, in particular, indicated which categories of persons were liable to have their telephone tapped: the persons concerned had to have taken part in an international telephone conversation via satellite connections or radio relay links (or also via fixed telephone lines in the case of monitoring to avert an armed attack on Germany, in accordance with section 3(1), point 1). In addition, the persons concerned either had to have used catchwords capable of triggering an investigation into the dangers listed in section 3(1), points 1-6, or had be foreign nationals or companies whose telephone connections could be monitored deliberately in order to avoid such dangers (section 3(2)).

98. As to the limit on the duration of telephone tapping, the Court notes that pursuant to section 5 of the G 10 Act (which was not amended by the 1994 Fight against Crime Act), the maximum duration of monitoring measures to be fixed in the order was three months; the implementation of the measure could be prolonged for a maximum of three months at a time as long as the statutory conditions for the order were met.

99. Moreover, the procedure to be followed for examining and using the data obtained was regulated in detail in section 3(3)-(5) of the amended G 10 Act. In particular, section 3(3) and (5) laid down limits and precautions concerning the transmission of data to other authorities; these were further strengthened by the Federal Constitutional Court in its judgment in the instant case.

100. As to the circumstances in which recordings may or must be erased or tapes destroyed, the Court observes that section 3 (6) and (7) and section 7(4) of the amended G 10 Act set out in detail the procedure for the destruction of data obtained by means of strategic monitoring. The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office.

101. Having regard to the foregoing, the Court concludes that the impugned provisions of the G 10 Act, seen in their legislative context, contained the minimum safeguards against arbitrary interference as defined in the Court's case-law and therefore gave citizens an adequate indication as to the circumstances in which and the conditions on which the public authorities were empowered to resort to monitoring measures, and the scope and manner of exercise of the authorities' discretion.

102. Therefore, the interferences with the applicants' right to respect for private life and correspondence as a result of the impugned provisions of the amended G 10 Act were "in accordance with the law" within the meaning of Article 8 § 2 of the Convention.

(b) Purpose and necessity of the interferences

103. The Government argued that the impugned interferences with the secrecy of telecommunications for the various purposes listed in section 3(1), second sentence, points 1-6, pursued a legitimate aim. They were necessary, in particular, in the interests of national security, public safety, the economic well-being of the country, and of the prevention of crime. The applicants did not comment on this issue.

104. The Court shares the Government's view that the aim of the impugned provisions of the amended G 10 Act was indeed to safeguard national security and/or to prevent crime, which are legitimate aims within the meaning of Article 8 § 2. It does not, therefore, deem it necessary to decide whether the further purposes cited by the Government were also relevant.

105. It remains to be ascertained whether the impugned interferences were "necessary in a democratic society" in order to achieve these aims.

106. The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security (see, *inter alia*, *Klass and Others*, cited above, p. 23, § 49; *Leander*, cited above, p. 25, § 59; and *Malone*, cited above, pp. 36-37, § 81). Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (see *Klass and Others*, cited above, pp. 23-24, §§ 49-50; *Leander*, cited above, p. 25, § 60; *Camenzind v. Switzerland*, judgment of 16 December 1997, *Reports* 1997-VIII, pp. 2893-94, § 45; and *Lambert*, cited above, p. 2240, § 31). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see *Klass and Others*, cited above, pp. 23-24, § 50).

107. The Court, while not losing sight of the legislative context, will first examine whether the interferences in question were proportionate to the legitimate aim pursued by each of the impugned provisions in turn, and will then make an overall assessment.

i. Strategic monitoring pursuant to section 3(1), taken in conjunction with section 1(1), point 2, of the amended G 10 Act (as modified by the Fight against Crime Act of 28 October 1994)

108. In the Government's submission, the impugned provision was necessary in a democratic society. It struck a proper balance between the public interest in averting the serious dangers listed in points 1-6 of section 3(1) and the interests of the persons concerned by the monitoring measures.

109. According to the Government, monitoring measures based on the G 10 Act had notably been necessary to combat international terrorism (point 2), by which democratic societies found themselves increasingly threatened, for instance by uncovering the command structure of Al-Qaida following the terrorist attacks of 11 September 2001. As regards international arms trafficking (point 3), it had, for example, been possible to prevent the export of dual-use goods into countries subject to an embargo and to improve export control with the help of strategic monitoring. It was impossible to counter these threats without resorting to strategic monitoring of telecommunications.

110. The Government argued that the way in which monitoring measures were taken and their extent were likewise not excessive. At the relevant time, merely some ten per cent of all telecommunications had been conducted by wireless means and had therefore been potentially subject to monitoring. In practice, monitoring was restricted to a limited number of foreign countries. By virtue of section 3(2), third sentence, the telephone connections of German nationals living abroad could not be monitored directly. The identity of persons telecommunicating could only be uncovered in rare cases in which a catchword had been used.

111. The applicant submitted that the scope of automatic surveillance under section 3(1) of the amended G 10 Act was far too wide, as there were no longer any geographical restrictions and as it was possible to identify persons and, if they were using mobile telephones, to analyse their movements. By virtue of section 3(2) of the amended G 10 Act, the second applicant could even be monitored deliberately. The Federal Intelligence Service was entitled to monitor all telecommunications within its reach without any reason or previous suspicion. Its monitoring powers therefore inhibited open communication and struck at the roots of democratic society. It was irrelevant whether or not it was already possible from a technical point of view to carry out worldwide monitoring.

112. In the applicant's view, these wide monitoring powers did not correspond to a pressing need on the part of society for such surveillance. There was no longer a threat of an armed attack on the Federal Republic of Germany by a foreign State possessing nuclear weapons, as there had been during the "Cold War". Nor was there any other comparable current danger to be averted. In particular, drug trafficking, counterfeiting of money and

money laundering or presumed dangers arising from organised crime did not constitute a danger to public safety sufficient to justify such an intensive interference with the telecommunications of individuals. The fact that interception was limited to content of "relevance for the intelligence service" ("*nachrichtendienstliche Relevanz*"), as a result of the decision of the Federal Constitutional Court, was not sufficient to constrain effectively the monitoring powers of the Federal Intelligence Service.

113. Moreover, the duty to have the interception of telecommunications authorised by the highest authorities of the *Länder* or a Minister of the Federal Government and the prior supervision of monitoring measures by an independent parliamentary committee did not avert the danger of abuse. It was likely that the interferences in question had been ordered in a result-oriented manner, notably because the excessive use of such measures, which, as a rule, remained secret, was unlikely to entail legal or political sanctions.

114. The Court is aware that the 1994 amendments to the G 10 Act considerably extended the range of subjects in respect of which so-called strategic monitoring could be carried out under section 3(1), the central provision at issue here. Whereas initially such monitoring was permitted only in order to detect and avert the danger of an armed attack on Germany, section 3(1) now also allowed strategic monitoring in order to avert further serious offences listed in points 2-6 of that section. Moreover, technical progress now made it possible to identify the telephone connections involved in intercepted communications.

115. While the range of subjects in the amended G 10 Act is very broadly defined, the Court observes that – just as under the G 10 Act in its initial version, which was at issue in its *Klass and Others* judgment – a series of restrictive conditions had to be satisfied before a measure entailing strategic monitoring could be imposed. It was merely in respect of certain serious criminal acts – which reflect threats with which society is confronted nowadays and which were listed in detail in the impugned section 3(1) – that permission for strategic monitoring could be sought. As regards the monitoring of telecommunications in order to avoid the counterfeiting of money abroad, the Federal Constitutional Court raised the threshold for interception by finding that such an offence could be serious enough to justify monitoring only if it was capable of threatening monetary stability in Germany. Surveillance could be ordered only on a reasoned application by the President of the Federal Intelligence Service or his deputy and if the establishment of the facts by another method had no prospect of success or was considerably more difficult. The decision to monitor had to be taken by the Federal Minister empowered for the purpose by the Chancellor or, where appropriate, by the highest authority of the *Länder* with the authorisation of the Parliamentary Supervisory Board. The Minister further had to obtain prior authorisation from the G 10 Commission or, in

urgent cases, *ex post facto* approval. Consequently, under the amended G 10 Act there was an administrative procedure designed to ensure that measures were not ordered haphazardly, irregularly or without due and proper consideration.

116. Moreover, the Court notes, with regard to the implementation of surveillance measures and the processing of the data obtained, that safeguards against abuse were spelled out in detail. Monitoring measures remained in force for a fairly short maximum period of three months and could be renewed only on a fresh application and if the statutory conditions for the order were still met. Monitoring had to be discontinued immediately once the conditions set out in the monitoring order were no longer fulfilled or the measures themselves were no longer necessary. As regards the examination of personal data obtained by the Federal Intelligence Service, the Federal Constitutional Court strengthened the existing safeguards by ordering that such data had to be marked as stemming from strategic monitoring and were not to be used for ends other than those listed in section 3(1). The transmission of data to the Federal Government and to other authorities under section 3(3) and (5) was also subject to conditions (which will be examined in more detail below). Moreover, the G 10 Act contained strict provisions concerning the storage and destruction of data. The responsibility for reviewing stored files on a six-month basis was entrusted to an official qualified to hold judicial office. Data had to be destroyed as soon as they were no longer needed to achieve the purpose pursued (see in more detail below, paragraphs 130-132).

117. As regards supervision and review of monitoring measures, the Court notes that the G 10 Act provided for independent supervision by two bodies which had a comparatively significant role to play. Firstly, there was a Parliamentary Supervisory Board, which consisted of nine members of parliament, including members of the opposition. The Federal Minister authorising monitoring measures had to report to this board at least every six months. Secondly, the Act established the G 10 Commission, which had to authorise surveillance measures and had substantial power in relation to all stages of interception. The Court observes that in its judgment in the *Klass and Others* case (cited above, pp. 24-28, §§ 53-60) it found this system of supervision, which remained essentially the same under the amended G 10 Act at issue here, to be such as to keep the interference resulting from the contested legislation to what was "necessary in a democratic society". It sees no reason to reach a different conclusion in the present case.

118. Consequently, strategic monitoring under section 3(1) was embedded into a legislative context providing considerable safeguards against abuse.

ii. Transmission and use of personal data pursuant to section 3(3), second sentence, of the G 10 Act, taken in conjunction with section 12 of the Federal Intelligence Service Act

119. The Government submitted that in a democratic society it was necessary for the Federal Intelligence Service to report to the Federal Government on the results of its monitoring measures in accordance with section 3(3), second sentence, of the amended G 10 Act, taken in conjunction with section 12 of the Federal Intelligence Service Act. This included the transmission of personal data which had to be marked as deriving from such measures. Otherwise, the Government would not be in a position to take effective measures to avert the dangers listed in section 3(1).

120. The applicants argued that there was no reason for the Federal Government to receive non-anonymous personal data obtained by the Federal Intelligence Service by means of the interception of telecommunications. The criminal prosecution of individuals was the task of the judiciary alone, and the transmission of such personal data could be abused for political aims.

121. The Court notes at the outset that in its judgment the Federal Constitutional Court found that the impugned provisions did not contain sufficient safeguards to ensure that the duty of the Federal Intelligence Service to report to the Federal Government, which included the transmission of personal data, was performed only for the purposes which had justified the collection of the data. That court ruled that, pending the entry into force of legislation in compliance with the Constitution, section 3(3), second sentence, could only be applied if the personal data contained in the report to the Federal Government were marked and remained connected to the purposes which had justified their collection.

122. The Court finds that the impugned provision, as amended and applicable following the judgment of the Federal Constitutional Court, laid down strict conditions with regard to the transmission to the Federal Government of data obtained by means of strategic monitoring. It is further convinced by the Government's argument that, in order effectively to avert the dangers listed in section 3(1), the transmission of personal – as opposed to anonymous – data might prove necessary. The additional safeguards introduced by the Federal Constitutional Court are appropriate for the purpose of limiting the use of the information obtained to what is necessary to serve the purpose of strategic monitoring.

iii. Transmission of personal data to the Offices for the Protection of the Constitution and other authorities and their use by these authorities in accordance with section 3(5) of the G 10 Act

123. In the Government's view, the transmission of the data in question was necessary in a democratic society for the prevention and prosecution of crime. It was a suitable means of achieving this aim, as it was the task of the recipient authorities to avert and investigate criminal offences. Taking into account the stipulations of the Federal Constitutional Court (in particular to the effect that transmission of data was permitted only if specific facts – as opposed to mere factual indications – had aroused the suspicion that one of the offences listed in section 3(3) was being planned or had been committed), the powers to transmit data were also not unreasonably wide. Moreover, there were sufficient procedural safeguards to guarantee that these requirements were complied with. The decision to transmit data was taken by a staff member qualified to hold judicial office and was reviewed by the G 10 Commission.

124. The applicants submitted that the transmission of personal data to, among other authorities, the Offices for the Protection of the Constitution was a further interference with their rights, which was not necessary in a democratic society. Despite the restrictions ordered by the Federal Constitutional Court, the scope of the cases in which the transmission of data was permitted remained wide and indeterminate. It was disproportionate to use information obtained by means of a serious interference with the secrecy of communications to combat a multitude of offences – some of which were rather petty – even if they were only in the planning stage. The obvious danger of abuse was not counterbalanced by sufficient procedural safeguards. Even though the decision to transmit data was taken by an official who was qualified to hold judicial office, there was no independent scrutiny, as the official in question was a staff member of the Federal Intelligence Service.

125. The Court finds that the transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings against those being monitored constitutes a fairly serious interference with the right of these persons to secrecy of telecommunications. It observes in this connection that the catalogue of offences for the investigation of which knowledge obtained by means of strategic monitoring could be used was considerably enlarged by the amendment of the G 10 Act at issue.

126. However, it notes that the use of information obtained by strategic monitoring to these ends was limited: personal data could be transmitted to other authorities merely in order to prevent or prosecute the serious criminal offences listed in section 3(3) of the amended G 10 Act.

127. Moreover, the Court observes that the Federal Constitutional Court found that the impugned section, in its version in force at the relevant time, interfered disproportionately with the secrecy of telecommunications as protected by the Basic Law. That court therefore ordered that, pending the entry into force of legislation in compliance with the Constitution, section 3(5) could only be applied and data be transmitted if specific facts – as opposed to mere factual indications – aroused the suspicion that someone had committed one of the offences listed in section 3(3). Furthermore, the transmission had to be recorded in minutes. Accordingly, that court again considerably strengthened the safeguards against abuse.

128. In addition, the decision to transmit data had to be taken by a staff member of the Federal Intelligence Service qualified to hold judicial office, who was particularly well trained to verify whether the conditions for transmission were met. Moreover, as clarified in the Federal Constitutional Court's judgment, the independent G 10 Commission's powers of review extended to verifying that the statutory conditions for data transmission were complied with.

129. In the light of the above, the Court takes the view that the interference with the secrecy of the communications made by persons subject to monitoring in accordance with the impugned provision was counterbalanced both by a reasonable limitation of the offences for which data transmission was permitted and by the provision of supervisory mechanisms against abuse.

iv. Destruction of personal data pursuant to section 3(6) and (7), taken in conjunction with section 7(4), of the G 10 Act

130. The Government took the view that the destruction of data was necessary in a democratic society because it limited interference with the secrecy of telecommunications to what was strictly required. Furthermore, pursuant to the order of the Federal Constitutional Court, data which were still needed for the purposes of court proceedings could not be destroyed immediately.

131. The applicants argued that destruction of data obtained by means of the interception of telecommunications likewise infringed their right to respect for their private life. Leaving the responsibility for the retention and destruction of files to the authorities involved entailed a great danger of abuse. The persons concerned by strategic monitoring were entitled to be informed about the destruction of personal data concerning them.

132. The Court notes in the first place that the impugned provisions, in providing for the destruction of personal data as soon as they were no longer needed to achieve their statutory purpose, and for the verification at regular, fairly short intervals of whether the conditions for such destruction were met, constituted an important element in reducing the effects of the interference with the secrecy of telecommunications to an unavoidable

minimum. Moreover, the Federal Constitutional Court ruled that data which were still needed for the purposes of court proceedings could not be destroyed immediately and that the supervisory powers of the independent G 10 Commission covered the whole process of using data, including their destruction. The impugned provisions consequently established further safeguards against abuse of the State's powers of surveillance.

v. Failure to give notice of restrictions on the secrecy of telecommunications pursuant to section 3(8) of the G 10 Act

133. In the Government's view, the provisions on notification were compatible with Article 8. As the purposes of strategic monitoring in accordance with section 3(1) would often be undermined if the persons concerned were subsequently informed about the measure, it was justified in such cases not to give any notification.

134. In the applicant's submission, the impugned section provided that notification had to take place only if it did not endanger the aim pursued by the restriction and the use of the data thus obtained. This exclusion of notification was too broad and entitled the authorities concerned not to give notification in order to avert dangers which were most unlikely to materialise.

135. The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Klass and Others*, cited above, pp. 26-27, § 57). However, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. Indeed, such notification might reveal the working methods and fields of operation of the Intelligence Service (see *Klass and Others*, cited above, p. 27, § 58, and, *mutatis mutandis*, *Leander*, cited above, p. 27, § 66). As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned (see, *mutatis mutandis*, *Leander*, cited above, p. 27, § 66, and *Klass and Others*, cited above, p. 27, § 58).

136. The Court notes that pursuant to section 3(8), any individuals monitored were to be informed that their telecommunications had been intercepted as soon as notification could be carried out without jeopardising the purpose of monitoring. Moreover, the Court observes that the Federal Constitutional Court again strengthened the safeguards against abuse

contained in the impugned provision by preventing the duty of notification from being circumvented; it found that in cases in which data were destroyed within three months there was justification for never notifying the persons concerned only if the data had not been used before their destruction. The Constitutional Court also clarified that the supervisory powers of the independent G 10 Commission extended to measures taken on the basis of section 3(8). In particular, the G 10 Commission had the power to decide whether an individual being monitored had to be notified of a surveillance measure (section 9(3) of the amended G 10 Act). The Court finds that the provision in question, as interpreted by the Federal Constitutional Court, therefore effectively ensured that the persons monitored were notified in cases where notification could be carried out without jeopardising the purpose of the restriction of the secrecy of telecommunications. It therefore contributed to keeping the interference with the secrecy of telecommunications resulting from the amended G 10 Act within the limits of what was necessary to achieve the legitimate aims pursued.

vi. Conclusion

137. In the light of the above considerations, the Court, having regard to all the impugned provisions of the amended G 10 Act in their legislative context, finds that there existed adequate and effective guarantees against abuses of the State's strategic monitoring powers. It is therefore satisfied that the respondent State, within its fairly wide margin of appreciation in that sphere, was entitled to consider the interferences with the secrecy of telecommunications resulting from the impugned provisions to have been necessary in a democratic society in the interests of national security and for the prevention of crime.

138. Accordingly, the applicants' complaints under Article 8 must be dismissed as being manifestly ill-founded, in accordance with Article 35 §§ 3 and 4 of the Convention.

C. Complaints under Article 10 of the Convention

139. In the first applicant's submission, certain provisions of the Fight against Crime Act, as interpreted and modified by the Federal Constitutional Court, amounted to a violation of freedom of the press. She complained about the same provisions of the Act as under Article 8 of the Convention (see above, paragraph 74). She relied on Article 10 of the Convention, which, in so far as relevant, reads:

> "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. ...

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

1. The parties' submissions

(a) The Government

140. In the Government's view, the impugned provisions of the amended G 10 Act did not interfere with the first applicant's freedom of expression. Strategic monitoring measures were not aimed at restricting the expression of opinions or the receipt of information, which would in fact have contravened the purposes of the surveillance. The secrecy of communications was protected by Article 8 alone.

141. The Government further argued that, even assuming that there had been an interference with the rights protected under Article 10, the interference had been justified within the meaning of paragraph 2 of that Article. It had been prescribed by law and was necessary in a democratic society. The Government referred to their submissions regarding Article 8 in that connection.

(b) The first applicant

142. The first applicant submitted, in particular, that the impugned monitoring powers under section 3(1) of the amended G 10 Act prejudiced the work of journalists investigating issues targeted by surveillance measures. She could no longer guarantee that information she received in the course of her journalistic activities remained confidential. Section 3(1) of the amended G 10 Act did not sufficiently protect journalists' communications and therefore disregarded the importance of a free press in a democratic society.

2. The Court's assessment

(a) Whether there was an interference

143. The Court reiterates that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance. The protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result the vital public-watchdog role of the press may be undermined**,** and the ability of the press to provide accurate and reliable information be adversely affected

(see, *inter alia*, *Goodwin v. the United Kingdom*, judgment of 27 March 1996, *Reports* 1996-II, p. 500, § 39, and *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 46, ECHR 2003-IV).

144. The Court further refers to its above findings under Article 8 to the effect that legislation permitting a system for effecting secret surveillance of communications involves a threat of surveillance in respect of persons such as the first applicant, who sufficiently substantiated her argument that that legislation could be applied to her. This threat necessarily strikes at the freedom of communication between users of telecommunications services and therefore amounts in itself to an interference with the exercise of the applicant's rights under Article 8, irrespective of any measures actually taken against her.

145. In the Court's view, this finding must be applied, *mutatis mutandis*, to the first applicant's right, in her capacity as a journalist, to freedom of expression as guaranteed by Article 10 § 1. The applicant communicated with persons she wished to interview on subjects such as drugs and arms trafficking or preparations for war, which were also the focus of strategic monitoring. Consequently, there was a danger that her telecommunications for journalistic purposes might be monitored and that her journalistic sources might be either disclosed or deterred from calling or providing information by telephone. For similar reasons to those set out in respect of Article 8, the transmission of data to other authorities, their destruction and the failure to notify the first applicant of surveillance measures could serve further to impair the confidentiality and protection of information given to her by her sources.

146. The Court therefore accepts that the impugned provisions interfered with the first applicant's freedom of expression.

(b) Whether the interference was justified

147. The Court, for the reasons set out in connection with Article 8, finds that the interference with the applicant's right to freedom of expression was prescribed by law, since it resulted from the impugned provisions of the amended G 10 Act, an Act passed by Parliament and applicable in the manner set out by the Federal Constitutional Court in its judgment of 14 July 1999.

148. The Court also finds that the interference pursued a legitimate aim, namely, the protection of the interests of national security and/or the prevention of crime.

149. In examining whether the interference was "necessary in a democratic society", the Court reiterates that, having regard to the importance of the protection of journalistic sources for the freedom of the press in a democratic society, an interference cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest. In reviewing the decisions taken – or

provisions enacted – by national authorities exercising their power of appreciation, the Court must look at the "interference" complained of in the light of the case as a whole and determine whether it was proportionate to the legitimate aim pursued and whether the reasons adduced by the national authorities to justify it were "relevant and sufficient" (see, *inter alia*, *Goodwin*, cited above, pp. 500-01, §§ 39-40, and *Roemen and Schmit*, cited above, § 46).

150. The Court notes at the outset that the Federal Constitutional Court found that the two impugned provisions concerning transmission to other authorities of data obtained by means of strategic monitoring, namely section 3(3) and (5), infringed the freedom of the press as protected by Article 5 § 1, second sentence, of the Basic Law. In order to ensure that data were used only for the purpose which had justified their collection, it ordered, in particular, that section 3(3) could be applied only if the personal data transmitted to the Federal Government were marked and remained connected to the purposes which had justified their collection. As regards the transmission of data to the authorities listed in section 3(5), the court laid down stricter conditions for transmission by ordering that there had to be specific facts arousing a suspicion that someone had committed one of the offences listed in section 3(3) and that the transmission had to be recorded in minutes. It stressed that such safeguards could also ensure that the Federal Intelligence Service took into account the important concerns of non-disclosure of sources and confidentiality of editorial work protected by the freedom of the press enshrined in Article 5 § 1 of the Basic Law.

151. The Court observes that in the instant case, strategic monitoring was carried out in order to prevent the offences listed in section 3(1). It was therefore not aimed at monitoring journalists; generally the authorities would know only when examining the intercepted telecommunications, if at all, that a journalist's conversation had been monitored. Surveillance measures were, in particular, not directed at uncovering journalistic sources. The interference with freedom of expression by means of strategic monitoring cannot, therefore, be characterised as particularly serious.

152. It is true that the impugned provisions of the amended G 10 Act did not contain special rules safeguarding the protection of freedom of the press and, in particular, the non-disclosure of sources, once the authorities had become aware that they had intercepted a journalist's conversation. However, the Court, having regard to its findings under Article 8, observes that the impugned provisions contained numerous safeguards to keep the interference with the secrecy of telecommunications – and therefore with the freedom of the press – within the limits of what was necessary to achieve the legitimate aims pursued. In particular, the safeguards which ensured that data obtained were used only to prevent certain serious criminal offences must also be considered adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum.

In these circumstances the Court concludes that the respondent State adduced relevant and sufficient reasons to justify interference with freedom of expression as a result of the impugned provisions by reference to the legitimate interests of national security and the prevention of crime. Having regard to its margin of appreciation, the respondent State was entitled to consider these requirements to override the right to freedom of expression.

153. The Court concludes that the first applicant's complaints under Article 10 of the Convention must be dismissed as being manifestly ill-founded, in accordance with Article 35 §§ 3 and 4 of the Convention.

D. Complaints under Article 13 of the Convention

154. In the applicants' view, certain provisions of the Fight against Crime Act amending the G 10 Act, as interpreted and modified by the Federal Constitutional Court, violated their right to an effective remedy. They complained, in particular, about the destruction of personal data (section 3(6) and (7), taken in conjunction with section 7(4), of the G 10 Act), the failure to receive notice of restrictions on the secrecy of telecommunications (section 3(8) of the G 10 Act), and the exclusion of judicial review of monitoring measures (section 9(6), taken in conjunction with section 3(1)). They submitted that these measures prevented them from lodging an effective complaint with the national courts about violations of their rights under Articles 8 and 10 of the Convention. They relied on Article 13 of the Convention, which provides:

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

155. According to the Court's case-law, Article 13 applies only where an individual has an "arguable claim" to be the victim of a violation of a Convention right (see *Boyle and Rice v. the United Kingdom*, judgment of 27 April 1988, Series A no. 131, p. 23, § 52; *Voyager Limited v. Turkey* (dec.), no. 35045/97, 4 September 2001; *Ivison v. the United Kingdom* (dec.), no. 39030/97, 16 April 2002; and *Petersen v. Germany* (dec.), nos. 38282/97 and 68891/01, 12 January 2006).

156. The Court has found that the substantive complaints under Articles 8 and 10 of the Convention are manifestly ill-founded. For similar reasons, the applicants did not have an "arguable claim" for the purposes of Article 13, which is therefore not applicable to their case. It follows that this part of the application is also manifestly ill-founded within the meaning of Article 35 § 3 of the Convention and must be rejected pursuant to Article 35 § 4.

For these reasons, the Court by a majority

Declares the application inadmissible.

Vincent BERGER
Registrar

Boštjan M. ZUPANČIČ
President