H e a d n o t e s

to the judgement of the First Senate of 14 July 1999

- 1 BvR 2226/94 -

- 1 BvR 2420/95 -

- 1 BvR 2437/95 -

1. **Article 10 of the *Grundgesetz* (Basic Law) not only provides protection from the state taking note of telecommunications contacts. Its protection also extends to the procedures by which information and data are processed following permissible acts of taking note of telecommunications contacts, and it extends to the use that is made of the obtained knowledge.**

2. **The territorial scope of protection of telecommunications privacy is not restricted to the domestic territory. Rather, Article 10 of the Basic Law is also applicable if an act of telecommunication that takes place abroad is, due to the fact that it is screened and evaluated on the domestic territory, sufficiently linked with domestic action of the state.**

3. **Article 73 no. 1 of the Basic Law grants the Federal government the competence to regulate the screening, utilisation and transfer of telecommunications data by the *Bundesnachrichtendienst* (Federal Intelligence Service). On the other hand, Article 73 no. 1 of the Basic Law does not entitle the Federal parliament to grant the Federal Intelligence Service powers that are aimed at the prevention or prosecution of criminal offences as such.**

4. **Whereas the parliament empowers the Federal Intelligence Service to conduct telecommunications monitoring that encroaches upon telecommunications privacy, Article 10 of the Basic Law obliges the Federal Intelligence Service to take precautionary measures against the dangers which result from the collection and utilisation of personal data. These precautionary measures include, in particular, that the use of obtained knowledge be bound to the objective that justified the collection of the data in the first place.**

5. **The competence of the Federal Intelligence Service under § 1 and § 3 of the G 10 Act to monitor, record and evaluate the telecommunications traffic for the timely recognition of specified serious threats to the Federal Republic of Germany from abroad and for the information of the Federal government is, in principle, consistent with Article 10 of the Basic Law.**

6. **The transfer of personal data that the Federal Intelligence Service has obtained from telecommunications monitoring for its own objectives to other government authorities is consistent with Article 10 of the Basic Law; it must, however, comply with the following prerequisites: (1) the data is necessary for the receiving agency's objectives; (2) the requirements placed on changes of objective as set forth in BVerfGE (Decisions of the Federal Constitutional Court) 65, p. 1 (at pp. 44 *et seq.*, 62) are met; and (3) the statutory thresholds for transfer comply with the principle of proportionality.**

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 2226/94 -
- 1 BvR 2420/95 -
- 1 BvR 2437/95 -

Pronounced
14 July 1999
Krenitz
Regierungssekretärin
Registrar
of the Court Registry

IN THE NAME OF THE PEOPLE

In the proceedings

on

the constitutional complaints

1. of Professor Dr. K...,

- authorised representative: Lawyer Johannes Latz,
Merlostraße 4, Cologne -

against § 3.1(1) and § 3.1 sent. 2 nos. 2-6, §§ 3.3, 3.4, 3.5, 3.7 and 3.8 of Article 1 of the Act of 13 August 1968 referring to Article 10 of the Basic Law (*Bundesgesetzblatt* [BGBl, Federal Law Gazette] I, p. 949), as promulgated on 28 October 1994 under the name of *Verbrechensbekämpfungsgesetz* (1994 Fight against Crime Act) (BGBl I, p. 3186), as amended by the Act of 17 December 1997 (BGBl I, p. 3108),

- 1 BvR 2226/94 -,

2. a) of Dr. W... (Ms),

b) of Mr. S...,

- authorised representative: Professor Dr. Eggert Schwan,
Am Volkspark 33, Berlin -

against § 1.1, § 3.1, § 3.2(3), §§ 3.3-3.8, § 7.4, § 9.6 of Article 1 of the Act of 13 August 1968 referring to Article 10 of the Basic Law (BGBl I, p. 949) as promulgated on 28 October 1994 under the name of *Verbrechens-bekämpfungsgesetz* (1994 Fight against Crime Act) (BGBl I, p. 3186), as amended by the Act of 17 December 1997 (BGBl I, p. 3108),

- 1 BvR 2420/95 -,

3. a) of T... GmbH,

b) of Dr. R...,

- authorised representatives: Lawyers Johannes Eisenberg and partners, Görlitzer Straße 74, Berlin -

against § 3.1(1) and § 3.1 sent. 2 nos. 2-6, §§ 3.2-3.8 of Article 1 of the Act of 13 August 1968 referring to Article 10 of the Basic Law (BGBl I, p. 949) as promulgated on 28 October 1994 under the name of *Verbrechens-bekämpfungsgesetz* (1994 Fight against Crime Act) (BGBl I, p. 3186), as amended by the Act of 17 December 1997 (BGBl I, p. 3108),

- 1 BvR 2437/95 -,

the First Senate of the Federal Constitutional Court, with the participation of

Judges Papier (Vice-President),

Grimm,

Kühling,

Jaeger,

Haas,

Hömig, and

Steiner

issued the following

J u d g e m e n t

on account of the oral argument of 15 and 16 December 1998:

1. **§ 3.1(1) and § 3.1 sent. 2 no. 5, §§ 3.3, 3.4, 3.5(1), 3.7(1) and 3.8(2) as well as § 9.2(3) of the Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10) (G 10) (Act on the Restriction of the Secrecy of Mail, Posts and Telecommunications; Act referring to Article 10 of the Basic Law; G 10 Act) as promulgated on 28 October 1994 under the name of Gesetz zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) (Act amending the Criminal Code, the Code of Criminal Procedure and Other Acts; Fight against Crime Act-Bundesgesetzblatt [Federal Law Gazette] I, p. 3186), as amended by the Begleitgesetz zum Telekommunikationsgesetz (BegleitG, Companion Act of the Telecommunications Act) of 17 December 1997 (Bundesgesetzblatt I, p. 3108) are inconsistent with Article 10 of the Basic Law. Moreover, §§ 3.3(1), 3.4 and 3.5(1) of the G 10 Act are inconsistent with Article 5.1(2) of the Basic Law, and § 3.8(2) of the G 10 Act is inconsistent with Article 19.4 of the Basic Law as well.**

2. **Regarding the other constitutional complaints brought by the complainant in the first constitutional complaint (1), by the first of the two complainants bringing the second constitutional complaint (2a), and by both complainants bringing the third constitutional complaint (3a and 3b), they are rejected as being unfounded.**

3. **The claims raised by the second of the two complainants bringing the second constitutional complaint (2b) are dismissed as inadmissible.**

4. **The Federal Republic of Germany shall reimburse one half of the necessary expenses of the complainant bringing the first constitutional complaint (1), the first of the two complainants bringing the second constitutional complaint (2a), and both complainants bringing the third constitutional complaint (3a and 3b).**

G r o u n d s :

A.

The constitutional complaints concern the authority of the *Bundesnachrichtendienst* (Federal Intelligence Service) to monitor, record and evaluate telecommunications traffic and to transfer the data thus obtained to other public agencies. The constitutional complaints also challenge other regulations of the *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* (Act on the Restriction of the Secrecy of Mail, Posts and Telecommunications) as amended in 1994 by the *Verbrechensbekämpfungsgesetz* (1994 Fight against Crime Act). 1

I.

1. The *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* 2

(Gesetz zu Artikel 10) (G 10) (Act on the Restriction of the Secrecy of Mail, Posts and Telecommunications; Act referring to Article 10 of the Basic Law; the G 10 Act) of 13 August 1968 (BGBl I, p. 949) came into force after Article 10 of the Basic Law was amended, in the wake of the constitutionally permissible measures arising out of a state of emergency (*Siebzehntes Gesetz zur Ergänzung des Grundgesetzes* [Seventeenth Act to amend the Basic Law] of 24 June 1968, BGBl I, p. 709), and from the outset provided for the possibility of monitoring telecommunications (§ 1). Monitoring was permissible in two forms: “Monitoring of Individuals” and “Strategic Surveillance.” § 2 of the G 10 Act regulated the monitoring of individuals. According to § 2 of the G 10 Act, monitoring individuals was permissible if there were grounds to suspect that someone planned, was committing or had committed specified, especially serious criminal offences that threatened the existence of the Federal Republic of Germany or its democratic order. § 3 of the G 10 Act regulated the so-called strategic surveillance which served in particular to compile situation reports on the state of certain dangers threatening the Federal Republic of Germany.

The present proceedings are exclusively concerned with strategic surveillance. 3
Originally, strategic surveillance was only permissible, pursuant to § 3.1(2) of the G 10 Act (old version), to ensure the early detection of armed aggression aimed at the Federal Republic of Germany and to avert such aggression. Strategic surveillance was therefore geographically restricted to territories from which a risk of war emanated. Pursuant to § 3.1(1) of the G 10 Act (old version), these areas were determined by the responsible Federal Minister with the approval of a panel, created by § 9.1 of the G 10 Act, consisting of members of the *Bundestag* (the German Parliament). Pursuant to § 5.1-§ 5.3 of the G 10 Act (old version), the minister was also responsible for determining which specific telecommunications traffic links were subject to monitoring and the attending restriction on the right to telecommunications privacy. In this context, a telecommunications traffic link was understood to be the scheduled telecommunications traffic which takes place in both directions between two specified ports in a network such as a collective cable system between two secondary telecommunications exchanges that crosses a border. Such collective cable systems were normally designated by a specific identification number (cf. BVerfGE [Decisions of the Federal Constitutional Court] 67, p. 157 [at p. 174]). Pursuant to § 9.2(2) of the G 10 Act (old version), the G 10 Commission decided whether monitoring was necessary and permissible.

An essential feature of the monitoring permitted pursuant to § 3 of the G 10 Act (old 4
version) was that it was not aimed at individuals (nor was this possible, for technical reasons) but served to obtain non-personal intelligence to provide the Federal government with information concerning foreign and defence policy issues. To the extent that strategic surveillance resulted in the collection of personal data, *e.g.* due to the fact that the communications partners themselves disclosed their identities, such personal data, pursuant to § 3.2(1) of the G 10 Act (old version), could not be used to the detriment of the subjects of monitoring. The law provided two exceptions to this rule.

First, pursuant to sent. 2 of the provision, the ban on detrimental use did not apply if the subject's right to telecommunications privacy had been restricted pursuant to § 2 of the G 10 Act. Second, the ban on detrimental use did not apply if there were *tatsächliche Anhaltspunkte* (factual grounds) to suspect that one of the acts set forth in § 2 of the G 10 Act or in Article 138 of the *Strafgesetzbuch* (StGB, German Criminal Code) was planned or committed.

The original version of the law provided in § 5.5 that the persons who were subject to monitoring measures could not be informed of these measures. Enforcing the provisions of Article 10.2(2) and Article 19.4(3) of the Basic Law, which were incorporated into the Basic Law in 1968, § 9.5 of the G 10 Act barred legal actions against an order implementing and the execution of monitoring. The Federal Constitutional Court determined that these provisions were consistent with Article 79.3 of the Basic Law, but declared § 5.5 of the G 10 Act void to the extent that this section prohibited notifying the subject of monitoring that such monitoring had taken place even if the objective of the monitoring would not be jeopardised by the notification. (BVerfGE 30, p. 1, [at p. 3]). As a result, the parliament provided, in the amended § 5.5 of the G 10 Act, for the notification of the subject of monitoring that such monitoring had taken place if the objective of the monitoring would not be jeopardised by the notification. After being notified of the monitoring, it was, pursuant § 5.5(4) of the G 10 Act, left to the discretion of the subject of the monitoring to take legal action. In the case of strategic surveillance, the Federal Constitutional Court did not regard it as necessary to notify the subject of the collected data of the monitoring if the supervision of the monitoring was ensured by independent state agencies and subsidiary agencies (cf. BVerfGE 67, p. 157 [at pp. 183 *et seq.*]). 5

2. The *Gesetz zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz)* (Act amending the Criminal Code, Code of Criminal Procedure and Other Acts [1994 Fight against Crime Act]) of 28 October 1994 (BGBl I, p. 3186), amended the G 10 Act in several respects. The reason given in support of the amendments was that they were intended to make it possible to monitor international telecommunications traffic in order to track the following spheres: international terrorism, the smuggling of narcotics to Germany, illegal trade in weapons of war, and international money laundering and counterfeiting activities. All of these activities, it was represented, increasingly threatened the security and the functioning of the state and the safety of the citizenry. The monitoring was intended to empower the responsible security authorities to prevent, resolve and prosecute criminal offences (cf. the statement in support of the bill, introduced to the *Bundestag* by the CDU/CSU and F.D.P. parliamentary groups; *Bundestagsdrucksache* [BTDrucks, Records of the *Bundestag*] 12/6853, p. 42). 6

The amendments expanded the objectives that justify monitoring pursuant to § 3.1(2) of the G 10 Act. In addition to the threat of armed aggression (no. 1), the amendments take up five more threats which result from different criminal activities and which bear a relation to foreign countries. These threats were specified as fol- 7

lows: international terrorist attacks (no. 2), international proliferation of weapons of war and of the trade in conventional arms (no. 3), importing narcotics into the Federal Republic of Germany (no. 4), counterfeiting committed abroad (no. 5) and money laundering in connection with the acts set forth under nos. 3 to 5 (no. 6).

However, as regards the newly added objectives that justify the collecting of information, monitoring was limited to wireless international telecommunications traffic, which was not technically developed at the time the original G 10 Act was enacted (§ 3.1[1] of the G 10 Act). Line telecommunications links may only be monitored to the extent that the risk of a war of aggression is concerned (§ 3.1[3] of the G 10 Act). The geographic range of monitoring was also expanded by the newly introduced threats under nos. 2 to 6. Whereas before, a risk of war was expected to emanate only from the territory of the Warsaw Pact, the new threats are not restricted to a single territory. 8

Moreover, the amendments result in an increase in the number of persons affected by monitoring. The targeted screening of individual telecommunications subscriber lines is prohibited under § 3.2(2) of the G 10 Act. Pursuant to § 3.2(1) of the G 10 Act, the selection of a telecommunications subscriber line for monitoring is to be made by means of search concepts which are intended and suitable for the resolution of issues arising out of one of the enumerated threats specified in the order establishing the restriction. However, pursuant to sent. 3 of the provision, this limitation does not apply to foreign individual telecommunications subscriber lines belonging to foreigners. Their terminal numbers may be used as so-called formal search concepts. In reality, the possibility of establishing references, especially to the identity of individuals, increases with the amendments due to the fact that today it is, in principle, technically possible to identify the individual subscriber lines involved in a telecommunications contact. 9

To the extent that personal data is obtained by means of monitoring, the ban on detrimental use no longer applies. Pursuant to sentence of §§ 3.3(1) and 3.5(1) of the G 10 Act, the data must be transferred in full to the Federal and *Länder* (Federal state) *Verfassungsschutzbehörden* (authorities concerned with the protection of the Constitution), the *Militärischer Abschirmdienst* (Military Counter-Intelligence Service), the *Zollkriminalamt* (Office of Criminal Investigation in Customs Matters), the *Bundesausfuhramt* (Federal Export Authority), the public prosecutors' offices and the police authorities. The data is to be used for the prevention, resolution and prosecution of certain criminal offences, to the extent that this is required for the fulfilment of the missions of these agencies. The catalogue of criminal offences that justify the use of personal data has been expanded considerably by the amendments in comparison with the original version of the law (§ 3.3(1) of the G 10 Act). However, the use of personal data is still subject to the precondition that monitoring occurring pursuant to § 2 of the G 10 Act has been ordered specifically regarding the subject of the monitoring or that there are *tatsächliche Anhaltspunkte* (factual grounds) for suspecting that someone plans, is committing or has committed one of the specified criminal offences. 10

Finally, the duty to inform the subject of monitoring that personal data has been collected, which arises pursuant to § 3.8 of the G 10 Act, has been restricted by the rule that the duty to inform does not apply in the case of § 3 of the G 10 Act if the personal data resulting from telecommunications monitoring has been deleted by the Federal Intelligence Service within three months or by the receiving agencies within another three months (§ 3.8[2] of the G 10 Act). 11

In principle, the authority of the Federal Intelligence Service to monitor and record telecommunications comes from § 1.1 of the G 10 Act. This provision reads, in the version of the *Begleitgesetz* (Companion Act) to the Telecommunications Act that was amended on 17 December 1997 (BGBl I, p. 3108), as follows: 12

1.The Federal and Länder (Federal state) Verfassungsschutzbehörden (authorities concerned with the protection of the Constitution), the Militärischer Abschirmdienst (Military Counter-Intelligence Service) and the Bundesnachrichtendienst (Federal Intelligence Service) are, in order to ward off dangers which threaten the free democratic order, the existence or the safety of the Federal Republic of Germany or of one of the German Länder (Federal states) including the safety of the troops of the non-German states stationed in the Federal Republic of Germany which are party to the North Atlantic Treaty,

2.the Federal Intelligence Service, in the framework of its mission pursuant to § 1.2 of the BND-Gesetz (Federal Intelligence Service Act), the latter as well for the objectives set out in § 3.1 sent. 2 nos. 2-6, 15

shall be entitled to monitor and record telecommunications and also, in the cases covered by no. 1, to open and inspect the items which are subject to correspondence and posts privacy. 16

§ 3 of the G 10 Act, in the version that is relevant in this context, reads as follows.[1] 17

(1) Apart from cases dealt with in § 2, monitoring of international wireless telecommunications links pursuant to § 1 may be ordered by application of the Federal Intelligence Service, and such monitoring must be ordered by the Federal minister who is responsible pursuant to § 5 with the consent of the panel of parliamentarians created pursuant to § 9. Monitoring is only permissible to collect information about issues the knowledge of which is necessary for the timely recognition of the threat of 18

1.armed aggression aimed at the Federal Republic of Germany; 19

2.international terrorist attacks against the Federal Republic of Germany, 20

3.international proliferation of weapons of war as defined by the Gesetz über die Kontrolle von Kriegswaffen (Act on the Control of Weapons of War) as well as the threat of illegal foreign trade in goods, data processing programs and technologies 21

1. *After the end of the oral argument, § 3 of the G 10 Act was amended again by Article 2 of the Gesetz zur Änderung von Vorschriften über parlamentarische Gremien (Act Amending the Regulations on Parliamentary Panels) of 17 June 1999 (BGBl I, p. 1334).*

under the terms of Part 1 of the Export List (Annex AL to the Außenwirtschaftsverordnung [Foreign Trade and Payments Ordinance]) in cases of considerable importance,

4.the illegal introduction of a not insignificant quantity of narcotics from abroad into the territory of the Federal Republic of Germany, 22

5.counterfeiting committed abroad and 23

6.money laundering in connection with the acts set forth under nos. 3 to 5 24

and to confront these threats. In the cases covered by no. 1, restrictions of privacy under sent. 1 may also be ordered for line telecommunications links and traditional postal correspondence. 25

[…] 26-30

(4) The Federal Intelligence Service shall examine whether personal data obtained by from monitoring conducted pursuant to § 3.1 are required for the objectives set forth therein. 31

(5) The data obtained pursuant to § 3.1 shall be transferred in full, for the objectives indicated under § 3.3, to the extent that this is required for the fulfilment of the receiving agency's mission, to the Federal and Länder (Federal states) government authorities concerned with the protection of the Constitution, to the Military Counter-Intelligence Service, to the Office of Criminal Investigation in Customs Matters, to the Federal Export Authority, the public prosecutors' offices and, subject to the public prosecutor’s power to control the subject matter of the litigation, to the police authorities. The decision whether to transfer the data shall be taken by an official who is qualified to hold judicial office. 32

(6) If data obtained pursuant to § 3.1 is not or is no longer required for the objectives set forth therein and if the data is not to be transferred to other agencies pursuant to § 3.5, the documents referring to the data shall be destroyed immediately under the supervision of an official who is qualified to hold judicial office, and to the extent that it is stored in electronic files, it shall be deleted. A record of the destruction and deletion shall be kept. Every six months it shall be examined whether the conditions for destruction or deletion of data exist. 33

(7) The receiving agency shall examine if it needs the data, transferred pursuant to § 3.5, for the objectives set forth under § 3.3. If it does not need the data, it is to destroy the documents immediately. The destruction is not necessary if it is not possible, or if it is only possible with unreasonable effort, to separate the data from other information which is necessary to fulfil the respective tasks; the use of this data is impermissible. 34

(8) Those persons affected by the collection of data pursuant to § 3.1 shall be informed about the monitoring of their telecommunications contacts as soon as a threat to the objective of the monitoring and to the use of the obtained data can be excluded. The provision of this information can be excused if the data has been destroyed 35

1.by the Federal Intelligence Service within three months after it was obtained or 36

2.by the agencies, to whom it has been transferred pursuant to § 3.5, within three months after its reception. 37

The duty to inform the subject of the monitoring that monitoring has occurred is incumbent upon the Federal Intelligence Service, in the case of transfer pursuant to § 3.5 it is incumbent upon the receiving agency. 38

(9) Before its decision on the permissibility and necessity of monitoring pursuant to § 9.2, the Commission can give the Federal Data Protection Commissioner the opportunity to give an opinion as regards data protection. The opinion is given exclusively vis-à-vis the Commission. 39

(10) The body created pursuant to § 9.1 shall report to the Bundestag (German Parliament) once a year about the state of implementation of the measures set forth under §§ 3.1- 3.9. 40

§ 7.4 of the G 10 Act regulates the destruction of personal data obtained by means of measures set forth under § 2 and § 3 of the G 10 Act, § 9 of the G 10 Act regulates the control of the measures and the preclusion of the recourse to a court. § 9 of the G 10 Act reads as follows:[2] 41

(1) The Federal minister who, pursuant to § 5.1, is responsible for the ordering of monitoring shall inform, at intervals not greater than six months, a panel consisting of nine members of the Bundestag who are appointed by the Bundestag, about the status of and affairs related to the implementation of this law. 42

(2) The responsible Federal minister shall inform, on a monthly basis, a commission about the monitoring measures ordered before they are executed. In the case of imminent danger, the minister may order the execution of monitoring before the commission is informed. The commission shall decide, ex officio or on account of complaints, about the permissibility and necessity of monitoring. Any orders for monitoring which the commission declares impermissible or unnecessary shall be cancelled immediately by the responsible Federal minister. 43

(3) The responsible Federal minister shall inform the commission, on a monthly basis, about the information given to those persons affected by data collection (§ 5.5) or about the reasons that stand in the way of this information being given. If the commission considers it necessary to give information to those persons affected by data collection, the responsible Federal minister shall order that such information is to be given immediately. 44

(4) and (5) ... 45

2. *§ 9 was also amended after the end of the oral argument by Article 2 of the Gesetz zur Änderung von Vorschriften über parlamentarische Gremien (Act Amending the Regulations on Parliamentary Panels) of 17 June 1999 (BGBl I, p. 1334).*

(6) Apart from that, the recourse to a court to challenge monitoring orders issued pursuant to § 2 and § 3.1 sent. 2 no. 1 and to challenge the execution of such orders, shall be precluded. 46

3. The Federal Constitutional Court issued a temporary injunction order (BVerfGE 93, p. 181) on 5 July 1995 pursuant to an application of the complainant bringing the first constitutional complaint. Pursuant to the temporary injunction order, § 3.3(1) of the G 10 Act is to be applied temporarily on the condition that personal data obtained pursuant to monitoring conducted in accordance with § 3.1 may only be used if *bestimmte Tatsachen* (specific facts) form the basis of the suspicion that someone plans, is committing or has committed one of the criminal offences named in the provision. § 3.5(1) of the G 10 Act is to be applied temporarily on the condition that the data obtained pursuant to § 3.1 is transferred to the agencies named in the regulation only if specific facts form the basis of the suspicion that someone plans, is committing or has committed one of the criminal offences named in § 3.3 of the G 10 Act. 47

4. In accordance with the Act and the provisions resulting from the Federal Constitutional Court's temporary injunction order, the Federal Intelligence Service has been conducting telecommunications monitoring since 1 March 1996. Orders pursuant to the G 10 Act have been issued concerning the spheres of weapons proliferation (§ 3.1 sent. 2 no. 3) which entered into force on 1 March 1996, international terrorism (no. 2) with validity from 1 April 1996, international arms trade and arms production (no. 3) which entered into force on 1 May 1996 and international drug trade (no. 4) with validity from 1 September 1996. In this context, approximately 5,200 alerts during monitoring were selected and subsequently evaluated in the spheres of weapons proliferation and arms trade until August 1998. Seventeen alerts were transferred pursuant to § 3.5(1) of the G 10 Act. In all cases, the receiving agency was the Office of Criminal Investigation in Customs Matters. In the spheres of international terrorism and international drug trade, 204 alerts were evaluated. There were no transfers to other agencies. These figures also include alerts which result from the monitored telecommunications traffic supplied by foreign intelligence services which was evaluated by the Federal Intelligence Service to the extent permitted by law. Due to the poor results, the orders with respect to the threats of terrorism and drug trade were not renewed in spring 1998. 48

II.

1. The complainant bringing the first constitutional complaint (1 BvR 2226/94) challenges, in his application, the expansion of the Federal Intelligence Service's powers to monitor as set forth in § 3.1 sent. 2 nos. 2-6 of the G 10 Act. He also challenges the manner in which the duty to inform of such monitoring is regulated in § 3.8 of the G 10 Act. Pursuant to the grounds he raises in his constitutional complaint, the complainant also challenges: first, § 3.4 of the G 10 Act which concerns the Federal Intelligence Service's power to examine and evaluate (for its own objectives); and second, §§ 3.3, 3.5 and 3.7 of the G 10 Act which regulate the Federal Intelligence Services' 49

power to transfer data and the power of other agencies to examine, evaluate and make further use of personal data obtained on account of the Federal Intelligence Service's power to monitor.

The complainant gives the following reasons for bringing his constitutional complaint. The complainant claims that his fundamental right under Article 10 of the Basic Law will, in all probability, be affected because, as a participant in international telecommunications traffic, he will be monitored by the computer search that is conducted pursuant to § 3.1 of the G 10 Act without a concrete suspicion to justify the monitoring. He is a university lecturer focusing, *inter alia*, on criminal law in the field of narcotics. In connection with his work he maintains varied private and official contacts - also per telephone and per fax - to countries situated east and west of Germany. He cannot influence the route (line or wireless) which the act of telecommunication takes. The complainant argues that it must be possible to challenge the regulation itself, since he as an individual is not subject to monitoring on the basis of suspicion and, pursuant to the legal regulation, he is not informed of the fact that his telecommunications contacts are being monitored. 50

According to the complainant, the challenged Act violates his fundamental rights under Articles 10, 1.1 and 2.1 of the Basic Law. 51

The complainant alleges that every time he dials an international telephone number and the connection is established via satellite or radio, the content of the communication link may be screened for search concepts, pursuant to a secret order establishing a restriction of his privacy rights, without any actual suspicion that the complainant is engaged in illegal activity. If search terms are found, the communication may be recorded. The complainant accepts that the so-called strategic surveillance contributes intelligence details which provide general information on certain threatening situations. It is the complainant’s position, however, that the decisive aspect concerning the question whether monitoring constitutes an encroachment upon fundamental rights is that for this objective, many individual acts of communication are monitored. The complainant argues that this type of computer search is, in reality, carried out not only without any suspicion of a threat that is related to a specific perpetrator but even without any suspicion related to a specific criminal offence. 52

According to the complainant, the result of this scheme is, as becomes evident through the powers of transfer under § 3.5 of the G 10 Act, that the Federal Intelligence Service becomes an investigation agency authorised to investigate in anticipation of threats. In the complainant's view, the Federal Intelligence Service has acquired police and procedural powers to encroach upon fundamental rights. The statement in the official justification of the Act that claims that the competencies of the Federal Intelligence Service have not been expanded is, therefore, false. The complainant also alleges that it is incorrect to assume that in the course of surveillance, a distinction can be made between, on the one hand, threatening international situations in general and dangers arising from criminal offences committed by individuals 53

on the other hand. As threatening situations are not international in the narrow sense but result from offensive acts committed by individuals, both aspects form an integrated whole. Thus, in the complainant's opinion, the Federal Intelligence Service becomes, contrary to the competencies conferred upon it by law and contrary to the separation of competencies between the police and the secret services established by the Constitution, a secret police investigation agency concerned with internal security to such a degree that it encroaches upon fundamental rights.

As concerns the extent of monitoring, the complainant argues that it must be assumed that, contrary to the opinion of the Federal government, the numerous monitoring facilities for radio signals emitted by satellites, radio systems and microwave radio systems allow, in the case of fully automatic filtering of the recorded material, the comprehensive monitoring of all accessible international radio and telecommunications traffic operations. Whether this possibility will be realised only depends on the procurement of the required facilities and equipment. It is not possible to restrict the so-called strategic surveillance to specific threats, in relation to specified telecommunications links, whether defined locally or otherwise. 54

The complainant alleges that in the three-stage procedure set forth by the Federal government, which includes general screening (preliminary recording or buffering), term base inquiry and more detailed evaluation of the recorded material, each of the three stages shows in itself the characteristics of an encroachment upon fundamental rights. The two first stages of the complex of activities, which the complainant alleges to constitute an encroachment, namely (1) the screening and recording of the act of telecommunication and (2) the term base comparison, affect the holder of fundamental rights without any suspicion of a criminal offence or any threat emanating from that individual. The relevant law does not presuppose any further suspicion of a criminal offence or of a threat which goes beyond the general possibility that the sources of the threats indicated in the law make use of telecommunications technology. 55

The intensity of the encroachment upon fundamental rights is increased, according to the complainant, in the case of all acts of telecommunication which contain search terms. They are evaluated, *i.e.* surveyed with a view to their content, by the staff of the responsible agency. From the complainant's perspective, this procedure completely eliminates telecommunications privacy. The technical prerequisites for a computer-aided term base comparison, which the Act assumes, do not exist as yet. This means that it is not possible to enforce the Act in compliance with the Basic Law. Nor is evaluation motivated by suspicion. The use of a specific semantic system, which is applied as a search term comparison, cannot in itself establish a threat-related or criminal offence-related initial suspicion. The complainant contends that it is an inherent characteristic of the computer search method that it also extends to many holders of fundamental rights for whom there is no suspicion of illegal activity. The complainant argues that this type of search is based only on suspected threats. 56

According to the complainant, the challenged provisions violate the principle of pro- 57

portionality. The extension of the powers of monitoring so that they cover general crime risks is justified by invoking the special situation of a threat emanating from international organised crime. The parliament, however, has not substantiated the assumed threat. The complainant alleges that no evidence even suggests that this threat represents an equivalent to the danger posed by the threat of external, armed aggression. Certainly the parliament has the prerogative of assessment. In this case, however, the parliament has completely refrained from assessing the factual phenomena.

The complainant also alleges that it is doubtful whether the measures are suitable for the indicated objective, *i.e.* investigation in the sphere of dangerous organised crime. The success of the monitoring measures is jeopardised by the use of encryption systems. Necessity is also not sufficiently substantiated. Due to the especially high rank of Article 10 of the Basic Law as concerns the general right to personality, the standards for justifying the necessity of an encroachment upon that right must also be especially high (*Unerlässlichkeit*, imperativeness). According to the complainant, the Act does not take this into consideration. Under the law, not even the serious suspicion of a criminal offence or of a threat is required. The law does not contain any consideration for weighing the necessity of expanding the secret police powers of the Federal Intelligence Service to include such an encroachment upon fundamental rights against alternative possibilities of regulation which are consistent with the rule of law. 58

The complainant raises other concerns about the principle of proportionality, which requires, in the narrow sense, principles of encroachment on individual freedoms that are consistent with the rule of law. Examples of such principles of encroachment on individual freedoms, which have been found to be consistent with the rule of law, include: (1) the rule under police law that an investigation may be justified if someone is found to be a “peace breaker” or an “apparent peace breaker” *(Störer- oder Anscheinsstörerverantwortung)*; (2) the rule under the law of criminal procedure that an investigation may be justified if a person is suspected of a criminal offence *(strafprozessrechtliche Tatverdachtsverantwortung)*; and (3) the rule permitting an investigation pursuant to compulsory joint liability *(Aufopferungspflicht)* of non-peace breakers and non-suspects. The encroachment on fundamental rights that compulsory joint liability permits is restricted to what is necessary and its intensity is relatively insignificant. The constitutional limitations on the power of encroachment under classical police law and under the law of criminal procedure, in connection with the pursuit of the suspicion of a criminal offence or of a threat, can be categorised according to the above-mentioned principles. The complainant asserts that the prerequisites of a threat or of suspicion of a criminal offence are essential for encroachments of fundamental rights and constitute the fundamental distinction between a state governed by the rule of law and a totalitarian state that investigates at its discretion to the detriment of unsuspected citizens. 59

The complainant admits that recent regulations of police law provide powers of encroachment upon fundamental rights in cases of abstract threats. It is the complainant's position, however, that no provision goes as far as the challenged Act. By allowing a broad computer search of data that is not justified by a specific threat or suspicion of a specific criminal offence, the Act departs from the classic principles which justify encroachment upon fundamental rights under police law and under the law of criminal procedure. These classic principles, which are consistent with the rule of law, require that there must be either a threat (under police law) or the suspicion of a criminal offence (under the law of criminal procedure). Apart from the "categories of threat" designated by law, the challenged Act imposes no preconditions regarding threats or specified suspicions of criminal offences. Encroachments upon fundamental rights which are completely removed from the tangible suspicion of a criminal offence have hitherto always been regarded as unconstitutional. The affected holders of fundamental rights are affected to a more than insignificant degree. Rather, the complainant argues, the core content of the freedoms guaranteed by fundamental rights is continually diminished up to the point of abrogation. This violates the essential content of the fundamental right in question. 60

The complainant charges that the challenged Act also violates the basic principle of the separation of powers established by the principle of the rule of law. The complainant contends that the Act completely withdraws the activity of the Federal Intelligence Service from judicial control over its power to order monitoring, especially by extensively excusing the Federal Intelligence Service from the duty to inform those being monitored that the monitoring has taken place. To the extent that the law, in general practice, precludes subjects of data monitoring (who are not suspected of illegal activity) from being informed that the monitoring has taken place, the law violates Article 19.4 in conjunction with Article 10.2(2) of the Basic Law. 61

The complainant argues that the concrete extension of strategic surveillance to general threats connected with criminal offences is not covered by the exception to the guarantee of communications privacy provided by Article 10.2(2) of the Basic Law. Pursuant to its wording, its legislative history and its interpretation, the exception applies only to the protection of the free democratic basic order and to the protection of the existence or the security of a *Land* (Federal state). The departure from the principle of judicial review of executive acts has been permitted by the parliament to the extent that: (1) there is a factual reason for this which is free from arbitrariness; and (2) the principle of the separation of powers, with its mutual checks and balances, is observed. With a view to the strategic surveillance of the threat of foreign aggression it had been regarded as permissible to prefer, over the procedure that would have normally been required, *i.e.* control by the courts, control of surveillance by a so-called political entity. The parliament is not free to extend this control to other classes of threat, especially to general threats associated with crime. 62

The complainant charges that, apart from this, the Federal parliament does not have the legislative competence to transform the Federal Intelligence Service into, what in 63

reality amounts to, a Federal secret police agency that acts on the domestic level. The Federal Intelligence Service is not mentioned in the Basic Law's provisions establishing various Federal legislative competencies. The competence to establish the Federal Intelligence Service is normally attributed to the Federal parliament on the basis of Article 73 no.1 of the Basic Law [Subjects of exclusive legislative power]. However, if this article is applied, the complainant urges that the limitation that it contains must be respected as well. Due to this limitation, the Federal competence does not extend to the attribution of powers of encroachment, on the domestic level, that are factually incumbent on the police or that are incumbent on the criminal police. According to the complainant such attribution violates the constitutional obligation to separate police service and secret service, to the extent that this obligation has found expression in the constitutional competence provisions referring to the Federal Intelligence Service.

2. The complainants bringing the second constitutional complaint (1 BvR 2420/95), 2a and 2b respectively, additionally challenge: first, measures of strategic surveillance pursuant to §§ 1.1, 3.1.(1), § 3.1 sent. 2 no. 1 and § 3.1(3) of the G 10 Act; second, the destruction of collected data without the consent of those being monitored pursuant to §§ 3.6, 3.7(2), 3.7(3) and 7.4 of the G 10 Act; and third, the preclusion of the recourse to a court set forth in § 9.6 of the G 10 Act. The complainants also regard their rights under Article 10, Article 2.1 in conjunction with Article 1.1 and Article 19.4 of the Basic Law as being violated by the challenged provisions. The first of the two complainants bringing the second constitutional complaint also claims that her fundamental right to freedom of the press under Article 5.1(2) of the Basic Law is violated. 64

The first of the two complainants bringing the second constitutional complaint (2a) asserts that she is a free-lance journalist working for many German and foreign newspapers, radio and television stations. She investigates especially in the areas with which the monitoring activities of the Federal Intelligence Service are concerned. There is, therefore, a high degree of probability that words occur in her telephone and fax traffic that are used as search concepts and that result in the recording of her telecommunications traffic. The second of the two complainants bringing the second constitutional complaint (2b) is an Uruguayan citizen. He claims that he takes care of the telecommunications traffic of the first complainant (2a) when she is absent for professional reasons, and that he uses her subscriber lines as well as his own subscriber line for this objective. Article 10 of the Basic Law can also be invoked by foreigners as regards measures taken by the German public authority outside of Germany. 65

The constitutional complaint is, according to the complainants, admissible and well-founded also with respect to the claim that §§ 1.1, 3.1(1) and § 3.1 sent. 2 no. 1 of the G 10 Act are unconstitutional. The conditions under which the Federal Constitutional Court, in its decision of 20 June 1984 (BVerfGE 67, p. 157), declared such monitoring measures constitutional, no longer exist. Primarily, the complainants argue, the War- 66

saw Pact has been dissolved. Still, telecommunications monitoring continues and it is not restricted to specified telecommunications links. The complainants argue that the action of the Federal Intelligence Service's "electronic vacuum cleaner," which collects data from the air, cannot be delimited regionally and personally in the manner required by the Federal Constitutional Court's previous case-law. The recording device also registers information about the subscriber lines that are used and thus, the identity of those being monitored. § 3.2(3) of the G 10 Act explicitly allows the search terms to contain identification characteristics which result in a targeted monitoring of certain telecommunications subscriber lines if the prerequisites for monitoring set forth in the provision are not met. This, according to the complainants, makes it possible to monitor the subscriber line of the second complainant (2b) in a targeted way.

67 The complainants argue that the Federal Constitutional Court has regarded strategic surveillance as permissible only under the condition that it is not misused for objectives that were not intended by the parliament. The complainants claim that, according to the Federal Constitutional Court, such unintended objectives include monitoring individuals or monitoring to obtain information necessary for a timely recognition of and response to threats to the internal security of the Federal Republic of Germany. Such objectives, however, are pursued by the concept of strategic surveillance as revised by the *Verbrechensbekämpfungsgesetz* (1994 Fight against Crime Act), and according to the complainants, surveillance takes place in a targeted way in order to obtain intelligence for the objectives set forth in §§ 3.1(1) and 3.1(2) of the G 10 Act.

68 The complainants argue that while the 1994 Fight against Crime Act distinguishes between the objective of strategic surveillance and internal security objectives when obtaining intelligence, the use of the data is uniformly regulated in §§ 3.3-3.7 of the G 10 Act. Consequently, § 3.2 of the G 10 Act (old version) has been set aside. Under this now abandoned regime it was, in principle, impermissible to use the data obtained for strategic surveillance objectives to the detriment of individuals. The complainants allege that the law is no longer based on the concept of a singular function, but on the concept of obtaining and using the data for multiple purposes. This concept, however, has already been declared unconstitutional by the Federal Constitutional Court.

69 As regards § 3.1 sent. 2 nos. 2 to 6 and §§ 3.3 -3.7 of the G 10 Act, the constitutional complaint is, according to the complainants, also well-founded. The regulations regarding the encroachment upon telecommunications privacy are not only applied in the lead-up to criminal prosecution, but also in the lead-up to the resistance to threats to internal security. The Federal parliament does not have the competence to pass laws that seek to prevent the criminal offences set forth in § 3.3 of the G 10 Act as a precaution against those threats during the lead-up phase. Moreover, encroachments upon telecommunications privacy require, as a prerequisite, a concrete initial suspicion of a criminal offence or the evidence of a concrete threat and are only permissi-

ble as a last resort.

Moreover, the complainants claim that the regulation set forth in § 3.3(2) of the G 10 Act in conjunction with § 12 of the *Gesetz über den Bundesnachrichtendienst* (BNDG, Federal Intelligence Service Act) is unconstitutional. It permits the transfer of collected data to the identified authorities without any restriction concerning the objectives to which these authorities are allowed to receive and use the transferred information. The only certainty is that these objectives are added to the ones set forth in § 3.3(1) of the G 10 Act. The complainants argue that it cannot be inferred from the Federal Intelligence Service Act that there is a restriction of objectives for which the transferred data may be used. This applies to § 12 of the Federal Intelligence Service Act as well as to § 1.2 of the Federal Intelligence Service Act. The latter assigns the Federal Intelligence Service the task of obtaining and evaluating intelligence which is important for foreign and security policy for the Federal Republic of Germany. In the opinion of the complainants such a regulation does not meet the requirements of the constitutional principle of clarity. 70

The complainants argue that § 3.5 of the G 10 Act is unconstitutional because the Basic Law prohibits the delegation of police functions, *i.e.* criminal prosecution or discovering and resisting threats, to the agencies concerned with the protection of the Constitution, which are mentioned in Article 73 no. 10b and Article 87.1(2) of the Basic Law. 71

The complainants allege that §§ 3.6 and 3.7 as well as § 7.4 of the G 10 Act violate Article 19.4 of the Basic Law. These sections of the Act violate the right to informational self-determination, and the essential content of this right, established by Article 2.1 in conjunction with Article 1.1 of the Basic Law. According to the interpretation the complainants give the statute, if a public agency no longer needs data that it has obtained and wants to destroy it, this agency must put the data at the disposal of the subjects of telecommunications monitoring and, at this point in time at the latest, the agency must inform the subjects of monitoring about the encroachments upon their informational rights in order to allow the subjects of monitoring, at least at that point in time, to defend their rights and, should the need for this arise, to seek recourse to a court. Therefore, the destruction of data is only permissible if those about whom data has been collected have consented to the encroachment upon their informational rights that this destruction of data constitutes. If this consent is not given, the complainants argue, the data must be handed over to the subjects of telecommunications monitoring. 72

The complainants argue that, for the same reasons, it is unconstitutional that § 3.8 of the G 10 Act contains no obligation to inform the subjects of telecommunications monitoring that such monitoring has taken place. Any doubt the agencies might have whether notifying would jeopardise the objective of the monitoring or of the use of the data is recognised as legitimate by the law. This is due to an erroneous balancing of the opposed legal interests. The regulation of § 3.8(2) of the G 10 Act gives greater 73

consideration to practicability which cannot justify the violation of Article 19.4 of the Basic Law, and which constitutes a violation of the right to informational self-determination.

It is the complainants' position that § 9.6 of the G 10 Act is unconstitutional as it precludes the recourse to a court in cases involving measures of strategic surveillance. The legal protection provided by Article 19.4 of the Basic Law cannot be restricted by a law. Nor does this article contain any "*immanente Schranken*" [inherent limitations through other rights and constitutional principles protected by the Basic Law] which would have the same effect. Furthermore, the regulation violates Article 2.1 in conjunction with Article 1.1 of the Basic Law as it violates the principle of proportionality. No legitimate objective can be discerned which can justify such a restriction. 74

3. The complainants bringing the third constitutional complaint (1 BvR 2437/95), (3a) and (3b) respectively, challenge that § 3.1(1) and § 3.1 sent. 2 nos. 2-6 and §§ 3.2-3 8 of the G 10 Act violate Article 10, Article 2.1 in conjunction with Article 1.1, Article 5.1(2), Article 19.4, Article 20.2 and Article 73 nos. 1 and 10 of the Basic Law. 75

The first of the two complainants bringing the third constitutional complaint (3a) publishes the daily newspaper "die tageszeitung." This legal entity claims that it maintains correspondents' posts in many countries and co-operates with free-lance authors and other publishers all over the world. Its reporting focuses, *inter alia*, on the subjects of corruption, international terrorism, international trade in drugs and arms, money laundering, organised crime, intelligence service activities, plutonium smuggling and the transfer of money from the First to the Third World. 76

The second of the two complainants bringing the third constitutional complaint (3b) is a journalist who lives in Germany and Italy and has a permanent residence in each of the countries. He claims that he researches and publishes, *inter alia*, in the areas of international terrorism, international trade in drugs and arms, money laundering, organised crime and intelligence service activities. He has many contacts at home and abroad to persons who form part of the circles which could be considered subjects of monitoring measures. 77

As participants in international telecommunications traffic, both complainants argue that they are directly affected by the challenged regulations. In this context, the first complainant (3a) claims that it exchanges with the second complainant (3b) and with other German and foreign correspondents the results of research and insight that may contain search concepts and combinations of search concepts that result in monitoring by the Federal Intelligence Service. The second complainant (3b) alleges that he conducts research mainly from Italy and predominantly works for German publishing houses and newspaper publishers. As both complainants are not informed of specific acts of implementation of the regulation, *i.e.* of orders for monitoring and of the interception and recording of telecommunications traffic, they have to challenge the legal regulation directly and generally. 78

The complainants claim that the challenged regulations violate Article 10, Article 5.1(2), Article 2.1 in conjunction with Article 1.1, Article 19.4 and Article 20.2 of the Basic Law. Moreover, the complainants argue, the Act violates the regulation of legislative powers established in the Basic Law, because with this law, the Federal parliament is able to regulate domestic police tasks even though it has no legislative authority to do so. A result of comprehensive telecommunications monitoring conducted without an existing suspicion of illegal activity is that effective journalistic research in the specific areas is no longer possible, to the extent that it must be carried out by means of telecommunications traffic across the German borders. It is the concern of the complainants that journalistic projects, which in their preliminary or preparatory stages are the subject of discussions via telecommunications facilities, cannot take place without the Federal Intelligence Service knowing about them, as such long-distance communications will contain the search concepts and search concept combinations and thus trigger monitoring. Another result of the monitoring, the complainants assert, will be that informants will refuse to supply information by telephone and will no longer make appointments by telephone or fax. Research that concerns the activities of the Federal Intelligence Service or of other secret services is, for instance, doomed to failure from the outset as the Federal Intelligence Service can anticipate and prepare for such investigations with the assistance of the monitoring allowed by the challenged regulations. 79

The complainants assert that the revision of Article 3 of the G 10 Act also breaks with the long-standing principles in cases involving encroachments upon telecommunications privacy. In the future, people for whom there is absolutely no reason to suspect criminal activity may be affected by the system of electronic telecommunications monitoring. Even if the obtained data is not transferred to prosecuting agencies, the Federal Intelligence Service may, pursuant to § 3.3(2) of the G 10 Act in conjunction with § 12 of the Federal Intelligence Service Act, transfer personal data to the head of the Federal Chancellery and the Federal ministers in the framework of their competencies. The subject of telecommunications monitoring, on the other hand, has no right to be informed if the Federal Intelligence Service or the receiving agency have destroyed the data within three months after it was obtained. 80

The complainants assume that only the Federal Intelligence Service is able to develop the adequate search concepts and combinations of search concepts. Thus, the Federal Intelligence Service possesses a *de facto* power of definition that is not really effectively controlled by the G 10 Commission. According to the complainants, the new legal regulations also preclude an autonomous control by the Federal Data Protection Commissioner. The Federal Data Protection Commissioner cannot become active on his or her own initiative but only on behalf of the G 10 Commission and may only inform this Commission (§ 3.9 of the G 10 Act). 81

The complainants argue that the expansion of authority to monitor telecommunications out of concern for the threat of terrorism, of the proliferation of weapons of war, drug trade and money laundering also cannot be subsumed under the concept "to 82

protect ... the existence or security of the Federation or of a *Land*." For this reason, the Federal Chancellery as well as the Federal Ministry of the Interior, first believed that an amendment of Article 10.2 of the Basic Law was required to permit the expanded authority to monitor telecommunications traffic. The complainants note that the Committee on Legal Affairs of the *Bundestag* (German Parliament) concluded that the determination of the tasks connected with the "importance from the security policy point of view" set forth in § 1.2 of the BNDG also covers telecommunications monitoring abroad by electronic means in the areas of terrorism, trade in arms and drugs as well as money laundering. The objectives of § 1.2 of the BNDG, however, are not identical to the constitutional concept of protecting "the existence or security of the Federation or of a *Land*" in Article 10.2.2 of the Basic Law.

III.

Opinions regarding the constitutional complaints have been given by: (1) the Federal Minister of the Interior on behalf of the Federal government; (2) the government of the Free State of Bavaria (a state of the Federal Republic of Germany); (3) the Federal Data Protection Commissioner; and (4) the data protection commissioners of the *Länder* (states) Bavaria, Berlin, Brandenburg, Bremen, Hamburg, North Rhine-Westphalia, Saarland and Schleswig-Holstein. 83

1. The Federal Minister of the Interior, who included a report by the President of the Federal Intelligence Service with his opinion, regards the constitutional complaints as inadmissible and in any case as unfounded. 84

a) As regards the facts of the matter, the Federal Minister of the Interior explained that monitoring measures pursuant to the amended § 3.1(2) of the G 10 Act have taken place since 1 March 1996. They are based on rules that specify the telecommunications links which should be subject to strategic surveillance. These rules determine the states or crisis regions that are the starting-points or end-points of the surveyed telecommunications links. Within this framework the specific orders restricting telecommunications privacy and permitting monitoring are made. Essentially, the provisions contain the search concepts according to which the surveyed telecommunications contacts are selected. According to the Federal Minister of the Interior, everything has been done to reduce, to a minimum, the possibility that unrelated parties become subjects of monitoring. 85

The Federal Minister of the Interior explained that he has issued rules concerning the threat of weapons proliferation (no. 3) which refer to telecommunications links between Europe and the states of the Near and the Middle East and also between Europe and the states of North Africa; rules regarding international terrorism (no. 2), which are valid for the same area; rules concerning the drug trade (no. 4) for telecommunications links between Europe and Africa, South America, Central America and Asia. On the basis of these rules, orders restricting telecommunications privacy issued for a limited time have been made regarding weapons proliferation in the narrower sense (*i.e.*, of so-called A, B and C weapons) and trade in conventional arms 86

and weapons as well as international terrorism and drug trade. The Federal Minister of the Interior claimed that, through the orders restricting telecommunications privacy, the wide geographic range of the areas mentioned in the rules has been limited to only a few states.

87 The Federal Minister of the Interior explained that a list of search concepts is part of each restriction order. Formal search concepts (subscriber lines of foreigners or foreign companies in foreign countries, to the extent permitted pursuant to §§ 3.2[2] and 3.2[3] of the G 10 Act) as well as content-related search concepts (*e.g.* terms from arms technology or names of chemicals needed for the manufacturing of illegal drugs) have been used. For the identification of threats in the field of weapons proliferation, approximately 2,000 search concepts have been employed, in the field of conventional arms trade almost 1,000, in the field of terrorism about 500 and in the field of drug trade about 400. Due to the poor results in the fields of terrorism and the drug trade, these restriction orders were not renewed in 1998.

88 As part of his defence of the monitoring provisions the Federal Minister of the Interior explained that the screening of telecommunications contacts has been restricted from the legal as well as the technical and capacity perspectives. For legal reasons, telecommunications traffic within Germany and within foreign states as well as line-bound international traffic are exempt from monitoring. Technically, screening is primarily restricted by the fact that the Federal Intelligence Service can, in the case of telecommunications traffic via satellite, only survey the downlink to Germany, not the uplink from Germany to foreign countries. Telecommunications contacts via microwave can only be screened if the microwave line is situated near one of the few points from which screening takes place. A targeted observation of specific acts of communication cannot be performed because the transmission routes cannot be determined beforehand.

89 In his reply to the constitutional complaints the Federal Minister of the Interior explained that the capacity of the Federal Intelligence Service permits the screening of approximately 15,000 acts of telecommunication per day out of a total of approximately 8 million telecommunications contacts between Germany and foreign countries. The material and personal resources of the Federal Intelligence Service, however, are not sufficient to evaluate all contacts. According to the Federal Minister of the Interior, experience has shown that out of the total number of screened acts of telecommunication, approximately 700 fall under the area of application of the G 10 Act. Only these acts are selected with the help of the search concepts. About 70 of them are examined more closely by employees of the Federal Intelligence Service. Not more than 15 alerts per day are passed on to specialised staff for examination. Of all international telecommunications contacts with subscriber lines in Germany, less than 0.1 thousandth enter the automatic selection process and less than 0.01 thousandth receive the attention of the evaluation staff of the Federal Intelligence Service.

90 The Federal Minister of the Interior further argued that fully automatic evaluation on

the basis of the search concepts is only possible in the field of telex transmission. In the case of fax transmission, which has been a part of strategic surveillance only since October 1997, only the formal search concepts can be screened automatically, whereas content-based selection is carried out by Federal Intelligence Service staff. In telephone traffic, neither an automatic selection of a subscriber number nor an automatic selection of content is presently possible. In particular, voice recognition procedures are not yet sophisticated enough to allow their application by the Federal Intelligence Service. For this reason, screening based on voice recognition is presently carried out in only a few selected cases.

b) As regards the legal aspects of the matter, the Federal Minister of the Interior made the following arguments: 91

aa) The Federal Minister of the Interior argued that the constitutional complaints are inadmissible. The Federal Minister of the Interior claimed that strategic telecommunications surveillance does not constitute "monitoring" of the complainants' telecommunications traffic. The mere possibility that telecommunications traffic in which the complainants engage is covered by monitoring acts and not immediately discarded as irrelevant is not sufficient to assume that there is an increased probability of the complainants' fundamental rights being impaired. Moreover, the second of the three constitutional complaints (1 BvR 2420/95) is inadmissible because the complainants live abroad and the second of the two complainants bringing the second constitutional complaint (2b) is not a German citizen so that the territorial aspect of the possible encroachment upon telecommunications privacy, which is required for the protection of a fundamental right, is missing. The Federal Minister of the Interior argued that telecommunications surveillance measures taken by the Federal Intelligence Service that cover the telecommunications traffic of foreigners within foreign countries are not directed against individuals who are protected by Article 10 of the Basic Law. 92

It is true, in the opinion of the Federal Minister of the Interior, that telecommunications privacy, with respect to its application to individuals, certainly protects Germans and foreigners alike. This, however, neither constitutes a decision about the factual scope of protection provided by this fundamental right nor a decision about whether its protection also extends to acts of state power by the German authorities, and to the effects of those acts, that occur and arise outside the territorial scope of the Basic Law and beyond the territorial sovereignty of Germany. The protection of fundamental rights as against the power of the German state is not exclusively restricted to the German territory. The Federal Minister of the Interior asserted, however, that the facts that are to constitute an encroachment upon fundamental rights must nevertheless show a reference to the territory of the Federal Republic of Germany which justifies the need for protection. The Federal Minister of the Interior objected to the claim that the power of the German state is everywhere and indiscriminately bound to the fundamental rights, a claim that, in his opinion, does not have general recognition. 93

The Federal Minister of the Interior argued that the general principles concerning the 94

limitations on the applicability of the fundamental rights abroad allow the conclusion that telecommunications surveillance performed by the Federal Intelligence Service pursuant to § 3 of the G 10 Act does not fall under the provisions of Article 10 of the Basic Law to the extent that the surveillance covers telecommunications traffic within foreign countries. The applicability of the Basic Law is restricted to the German territory. Notwithstanding this rule, the fundamental rights also bind German state power to the extent that this power becomes effective abroad by virtue of international law or on account of a special permission by the foreign territorial state in question; and to the extent that the encroachment is based on the territorial sovereignty or the personal sovereignty of Germany. However, effects resulting from the exercise of German state power abroad that can neither be derived from territorial sovereignty nor from personal sovereignty cannot be resisted by invoking the fundamental rights enshrined in the Basic Law.

The Federal Minister of the Interior argued that the challenge raised by the second constitutional complaint (1 BvR 2420/95), which claims that § 3.1 sent. 2 no. 1 and that § 9.6 of the G 10 Act encroach upon fundamental rights, has been lodged too late. 95

bb) In any case, the constitutional complaints are, according to the Federal Minister of the Interior, unfounded. 96

The Federal Minister of the Interior explained in his submission that the legislative power of the Federal Republic flows from Article 73 no. 1 of the Basic Law. The competence for foreign affairs includes the competence to establish an intelligence service, to the extent that such a service becomes active abroad or its activities are directed towards foreign countries. The reference to foreign countries is assured in the 1994 Fight against Crime Act. § 1.1 no. 2 of the G 10 Act explicitly restricts the competencies to monitor and record telecommunications traffic pursuant to § 3.1 sent. 2 nos. 2-6 of the G 10 Act to the structure of tasks of the Federal Intelligence Service set forth in § 1.2 of the Federal Intelligence Service Act. Accordingly, the authority to monitor telecommunications traffic in § 3.1(2) of the G 10 Act refers to international telecommunications links. Based on the international character of the threats set forth under nos. 2, 3 and 6, and on account of the acts of aggression set forth under nos. 4 and 5 (which must originate or be committed in foreign countries) the Federal Minister of the Interior concludes that the new grounds restricting telecommunications privacy that are outlined in § 3.1 of the G 10 Act show the required factual reference to the authority conferred to the Federal Republic by Article 73 no. 1 of the Basic Law. 97

The Federal Minister of the Interior took the position that the provisions of the 1994 Fight against Crime Act do not confer any authority to the Federal Intelligence Service that is exclusively reserved by the Basic Law for the domestic police agencies. In this context, it need not be decided whether the Basic Law contains a constitutional principle that requires the separation between the police and the (domestic) intelligence services. In any case, the Federal Minister of the Interior asserted that the standards 98

promoted by the supporters of such a constitutional principle of separation are not violated. No organisational and institutional link between the Federal Intelligence Service and police agencies is established. No authority to encroach upon telecommunications privacy rights, which have been reserved for the police, have been conferred to the Federal Intelligence Service. The authority is, also in the framework of the monitoring objectives pursuant to § 3.1 sent. 2 nos. 2-6 of the G 10 Act, restricted to surveillance as regards foreign countries with intelligence service aims.

The Federal Minister of the Interior argued that the principle of separation between police and intelligence services is not circumvented by the obligation to transfer, pursuant to § 3.5 of the G 10 Act, the data that was obtained in accordance with § 3.1 of the G 10 Act. No general prohibition on co-operation and on the interchange of information can be inferred from the principle of separation. The objective of the separation is to prevent the combination of the intelligence services' knowledge, which goes far beyond the knowledge required by the police for the resistance of threats and for criminal prosecution, with the authority of the police. The Federal Minister of the Interior contends that the barriers resulting from this have been carefully observed when the provisions concerning data transfer were amended by §§ 3.3-3.5 of the G 10 Act. 99

The Federal Minister of the Interior claimed that the transfer of data takes place within the framework of the legal authority of the Federal Intelligence Service, and its prerequisite is a suspicion that is comparable, as regards the required degree of suspicion, to the initial suspicion under the terms of § 152.2 and § 160.1 *Strafprozessordnung* (StPO, Code of Criminal Procedure) and to the suspicion that is required for the undercover use of technical devices pursuant to the police laws of the *Länder* (states), and which goes beyond the required suspicion to the extent that it must refer to specific criminal offences. The Federal Minister of the Interior argued, however, that the principle of separation does not require that the Federal Intelligence Service transfer data to an agency of criminal prosecution only in cases in which the requirements for an order pursuant to § 100a of the Code of Criminal Procedure are fulfilled. The function of § 100a of the Code of Criminal Procedure is completely different from the principle of separation. § 100a deals with the question: under which preconditions may an encroachment upon telecommunications privacy take place for the objective of collecting evidence for a criminal procedure. The principle of separation, however, concerns the question of the required prerequisites that would allow information obtained by means of a (permissible) encroachment that has already taken place, to be used for objectives related to criminal proceedings or crime prevention. 100

The Federal Minister of the Interior asserted that the expansion of the grounds justifying orders restricting telecommunications privacy pursuant to § 3.1 sent. 2 nos. 2-6 of the G 10 Act has only changed: (1) the extent to which data may be obtained; and (2) part of the elements of a criminal offence that justify transfer pursuant to § 3.3 of the G 10 Act. The elements of a criminal offence partly correspond with the expanded grounds for orders restricting telecommunications privacy. To the extent that such parallels do not exist, this was already true, according to the Federal Minister of the 101

Interior, of § 3.2(2) of the G 10 Act (old version). This means that the legal structure of the G 10 Act has been preserved. The authority to transfer found in § 3.3 in conjunction with § 5 of the G 10 Act is based on the grounds set forth in § 3.1(2) of the G 10 Act that permit orders restricting telecommunications privacy. According to the Federal Minister of Interior, this means that nothing has changed in comparison to the old legislation.

The Federal Minister of the Interior further argued that the standard for the review of the constitutionality of the challenged regulations is the privacy of telecommunications enshrined in Article 10 of the Basic Law, which also provides protection against the use and transfer of data that were obtained by an encroachment upon this fundamental right. The Federal Minister of the Interior argued, however, that the fundamental right of the freedom of the press is not relevant in this context. The G 10 Act itself neither restricts the freedom of the press nor authorises such restrictions. It is certainly not impossible, but nevertheless rather remote, that telecommunications traffic associated with the field of journalism will be monitored with the help of the search concepts. To the extent that this should occur in exceptional cases, the use or transfer of such data is only permitted pursuant to the narrow scope of powers provided by § 3.3 and § 3.5 of the G 10 Act. The Federal Minister of the Interior claimed that when the law is applied in this respect, the meaning and scope of the freedom of the press must be given due consideration. 102

The Federal Minister of the Interior argued that § 3.1 sent. 2 no. 1 of the G 10 Act, which is challenged in the second constitutional complaint (1 BvR 2420/95), does not violate Article 10 of the Basic Law. The constitutional complaint misjudges the continuing importance of the state's efforts to provide for the national defence. According to the Federal Minister of the Interior, the constitutional complaint tries to deny the existence and even the possibility of a threatening situation as regards the national defence without being able to provide a reliable forecast in this respect. According to the Federal Minister of the Interior, the power to perform strategic surveillance continues to be meaningful and necessary even though the nature of threatening situations has changed. 103

The Federal Minister of the Interior took the position that § 3.1 sent. 2 nos. 2-6 of the G 10 Act and § 3.8 of the G 10 Act also do not violate the complainants' fundamental right under Article 10 of the Basic Law. By issuing the challenged regulations, the parliament has fulfilled the constitutional obligations of Article 10.2(1) of the Basic Law [which establishes that restrictions of the privacy of correspondence, posts and telecommunications may only be ordered pursuant to a law]. 104

The Federal Minister of the Interior argued that without changing the position and the aims of the Federal Intelligence Service, the 1994 Fight against Crime Act has expanded the objectives that are served by the Federal Intelligence Service's surveillance as well as the powers of the Federal Intelligence Service itself. The aspects in which the new objectives of encroachment exceed strategic surveillance as it existed 105

before also refer to fields of threat to the Federal Republic of Germany. According to the Federal Minister of the Interior, increasingly discernible threats to the state's safety and ability to function emanate from international terrorism, from illegal trade in the weapons of war, the drug trade to Germany and international money laundering.

Since 1990, the provisions in the fields of the *Außenwirtschaftsgesetz* (Foreign Trade and Payments Act) and of the *Kriegswaffenkontrollgesetz* (Act on the Control of Weapons of War) have been drastically tightened and control procedures have been expanded in order to be able to timely counteract rearmament abroad that proceeds with the help of German companies. In the opinion of the Federal Minister of the Interior, the Federal Intelligence Service's expanded authority in the area of telecommunications monitoring is necessary to fulfil its statutory mandate to monitor the field of weapons proliferation and in particular to provide the responsible German agencies with the relevant intelligence that is obtained. 106

As concerns weapons proliferation, the Federal Intelligence Service already engaged in telecommunications monitoring before the 1994 Fight against Crime Act came into force; monitoring precluded, however, telecommunications traffic which involved participants protected by Article 10 of the Basic Law. The Federal Minister of the Interior explained that it is an elementary foreign policy interest of the Federal Republic of Germany and also an elementary interest of its policy as a NATO member to be in a position to engage in its own monitoring of weapons proliferation activities. Otherwise, the Federal Republic of Germany might be reproached for deliberately turning a blind eye on such activities to facilitate lucrative export deals to German companies, for example. 107

The Federal Minister of the Interior argued that expanded strategic surveillance is, in its entirety as well as in its individual stages of procedure, suitable and necessary to achieve the aim of recognising and counteracting threats to the Federal Republic of Germany. Expanded strategic surveillance is also proportional. 108

The Federal Minister of the Interior noted that, due to the requirements placed on the search concepts and due to their selection and design, there is only a limited probability of becoming the subject of a restriction on the right to telecommunications privacy. To the extent that telecommunications traffic is temporarily recorded before the term base comparison, or the comparison with the search concepts cannot be performed automatically, the intensity of the encroachment upon fundamental rights is low. On the other hand, expanded strategic surveillance serves to avert threats to the Federal Republic of Germany that have an international aspect. The Federal Minister of the Interior took the position that the new aims of monitoring are similar to the ones pursued by conventional strategic surveillance. Certainly, expanded strategic surveillance is, to a greater extent than before, aimed at combating crime. This is only true, in the opinion of the Federal Minister of the Interior, with respect to threats to internal security if those threats first meet the standard that the Federal Republic of Germany is also confronted with them from outside. 109

The Federal Minister of the Interior also claimed that the parliament, with § 3.3 of the G 10 Act, has expanded within reasonable boundaries the catalogue of criminal offences for the prevention, resolution or prosecution of which the use personal data is permitted. § 3.3 of the G 10 Act is supposed to assure that intelligence from the newly added fields of monitoring can be used for the objectives set forth in § 3.3 of the G 10 Act. According to the Federal Minister of the Interior, the only real extension of this provision consists in incorporating § 264 of the *Strafgesetzbuch* (Criminal Code) and § 92a of the *Ausländergesetz* (Aliens Act) into the catalogue. As concerns their legal structure, § 3.1 of the G 10 Act makes reference to § 3.3 of the G 10 Act in the same way that the previous § 3.1(2) of the G 10 Act (old version) made reference to § 3.2 of the G 10 Act (old version). 110

The Federal Minister of the Interior also noted that the authority to use personal data for the prevention, resolution or prosecution of specified criminal offences, and to transfer it to the responsible agencies if necessary, is contingent upon the existence of *tatsächliche Anhaltspunkte* (factual grounds) for suspecting that someone is planning or committing or has committed one of the listed criminal offences. This is due to the fact that the Federal Intelligence Office is not a police agency that is entitled to intervene in the case of concrete threats to the public safety and order. The Federal Intelligence Office is also not a crime prosecution agency that is authorised to act if specific facts substantiate the suspicion that a criminal offence exists. Therefore, the Federal Minister of the Interior argued that the Federal Intelligence Service cannot be allowed to evaluate and further use personal data only under the restrictive prerequisite that specific facts justify the suspicion that one of the listed criminal offences exists. 111

The Federal Minister of the Interior argued that § 100a of the *Strafprozessordnung* (Code of Criminal Procedure) is not a suitable standard for evaluating the further use and transfer of personal data. This provision only serves the fight to repress crime. Expanded strategic surveillance, however, is supposed to facilitate the early detection of threats. This preventive aspect is taken up in § 3.3(1) of the G 10 Act as the provision is primarily aimed at criminal offences that are still in the planning phase or that are actually being committed at that respective moment. The fact that the further use and transfer of gathered personal data primarily serves a preventive function also becomes evident from the agencies that are entitled to receive data: the *Verfassungsschutzbehörden* (agencies entrusted with the protection of the Constitution), the *Militärischer Abschirmdienst* (Military Counter-Intelligence Service), the *Zollkriminalamt* (Office of Criminal Investigation in Customs Matters), the *Bundesausfuhramt* (Federal Export Authority) and the police. These agencies should receive personal data primarily in order to prevent and combat imminent criminal offences. 112

The Federal Minister of the Interior asserted that even if there are only factual grounds to suspect an imminent or continuing criminal offence, immediate transfer to the police must be permissible because everything must be done at the earliest possible stage to prevent the commission of the criminal offence. Otherwise, it probably 113

will, in many cases, be too late to prevent the criminal offence. However, in view of the necessary protection of high-ranking legal interests and safety interests, such delay is not acceptable, especially when taking the principle of proportionality into account.

As the Federal Intelligence Service is, when transferring personal data, bound to the standard that a temporary injunction order must exist, there are no figures that show how many transfers could have taken place if factual grounds to suspect a criminal offence were already sufficient to justify transfer of obtained data. However, there are greater possibilities of transfer if the thresholds are lower. As it is a typical feature of intelligence activities that information is only gathered on partial aspects of incidents, the phrase "*tatsächliche Anhaltspunkte*" (factual grounds) set forth in § 20 of the *Bundesverfassungsschutzgesetz* (BVerfSchG, Federal Constitution Protection Act), in § 9.3 of the Federal Intelligence Service Act (BNDG) and in § 11.2 of the *Gesetz über den Militärischen Abschirmdienst* (Military Counter-Intelligence Service Act) has been deliberately chosen to designate the threshold for transfer. According to the Federal Minister of the Interior, the decisive question is always how many partial aspects of an incident must be covered before surveillance in the lead-up to a criminal offence is completed and investigation can be taken up by the police or the public prosecutor. 114

On the basis of *tatsächliche Anhaltspunkte* (factual grounds), the Federal Intelligence Service would transfer its intelligence earlier than under the prerequisite relying on the standard of a suspicion substantiated by specific facts. For instance, the supply of "dual-use" goods violates the Foreign Trade and Payments Act and the Act on the Control of Weapons of War only if the requirements for permission stipulated in these Acts have been disregarded. In such cases, only the Office of Criminal Investigation in Customs Matters or the Federal Export Authority can ascertain if the law has been violated by comparing the permits that have been issued. Only such a comparison may provide "*bestimmte Tatsachen*" (specific facts) to justify the suspicion that the supplier plans, is committing or has committed one of the criminal offences listed in § 3.3 of the G 10 Act. 115

The Federal Minister of the Interior also argued that taking § 100a of the Code of Criminal Procedure as a standard is problematic because this approach confers examination criteria to the Federal Intelligence Office that are reserved to the judiciary or at least to the public prosecutors' function. If the examination activities of the Federal Intelligence Office took such a shape, this would run counter to the very endeavour to deny the Federal Intelligence Office the authority to encroach upon the fundamental right to privacy that is reserved for the police, and more importantly, the authority that is reserved for the public prosecutors or the judiciary. For the wording of § 3.3(1) of the G 10 Act, the parliament took § 2.1 of the G 10 Act, § 10.1 of the BVerfSchG, and § 20.1 no. 7 of the *Stasi-Unterlagengesetz* (Stasi [GDR secret service] Records Act) as models. 116

The Federal Minister of the Interior concluded in his submission to the Court that the 117

way in which the duties to inform are regulated in § 3.8 of the G 10 Act does not violate Article 19.4 of the Basic Law.

The Federal Minister of the Interior accepted that Article 19.4(1) of the Basic Law can require that the state inform the person whose telecommunications privacy rights have been secretly restricted of the encroachment because the guarantee of recourse to a court is the citizens' central means of protecting their rights and because this guarantee depends on whether the citizen knows that his or her rights have been violated. The Federal Minister of the Interior argued, however, that this duty to inform does not have unlimited application. It is explicitly restricted by the Constitution itself, in Article 19.4(3) in conjunction with Article 10.2(2). The Federal Minister of the Interior concluded that the prerequisites for the subsequent provision of information regarding an encroachment of telecommunications privacy, which have been established by the Federal Constitutional Court, are fulfilled by § 3.8 of the G 10 Act. 118

The Federal Minister of the Interior argued that even when it is taken into account that the objectives for which strategic surveillance is permitted have been expanded, which, as a consequence, involves to an increased extent the defence against and the prosecution of certain criminal offences and, in this context, the recording of personal data, Article 19.4 of the Basic Law is not violated. The legal interests protected by § 3.1 sent. 2 nos. 2-6 of the G 10 Act carry such a weight that in the cases covered by § 3.8(1) of the G 10 Act the citizens' legal protection will have to be subordinated, at least temporarily. § 3.8(1) of the G 10 Act restricts the monitored persons' factual possibility of obtaining recourse to a court only to the extent required for achieving the objective of the Act. In the period of time during which the subject of telecommunications monitoring may not be informed of the surveillance, the monitoring is controlled by the independent commission established by § 9 of the G 10 Act. 119

The Federal Minister of the Interior also asserted that § 3.8(2) of the G 10 Act is consistent with Article 19.4 of the Basic Law because the encroachment upon Article 10 of the Basic Law does not result in any consequences for the person being monitored and because the intensity of the encroachment is low. The Federal Minister of the Interior suggested that the special provisions that restrict the duty to inform the monitored persons are the appropriate result of the parliament’s weighing of interests and a fulfilment of its duty to strike a balance between the following interests: (1) the individual's interest in protection; (2) the safeguarding of the objective of the restriction on the right to telecommunications privacy and of the use of the information obtained thereby; and (3) the Federal Intelligence Service’s mission and its manner of functioning. The Federal Minister of the Interior argued that the mere fact that a public agency has obtained knowledge of personal data does not trigger the duty to inform the person being monitored of the encroachment, which derives from the *allgemeines Persönlichkeitsrecht* (general right to personality) or from the guarantee of legal protection provided by the recourse to a court. The public agency's duties to inform are not supposed to extend so far as to make it impossible to exercise public functions. 120

The Federal Minister of the Interior also asserted that the deletion periods provided by the Act take into account, on the one hand, the monitored person's interest in the shortest possible period during which his or her personal data is stored; and on the other hand, the need of combating the serious threats in question by comprehensively ascertaining the facts. The Federal Minister of the Interior noted that, due to the considerable volume of telecommunications traffic monitored every day and the need for a careful selection, it was necessary to concede the Federal Intelligence Service a period of at least three months to ascertain the relevance of the data. This applies, in a similar way, to the agencies that are provided with intelligence and facts from telecommunications monitoring for further processing. Also, these agencies must check the relevance of the data and, for doing so, they must pursue the investigations that are necessary for ascertaining the facts. This is not possible in a period of time shorter than the one set forth in the Act. 121

The Federal Minister of the Interior argued that in the cases in which no information pursuant to § 3.8(2) of the G 10 Act is provided, neither the principle of the rule of law nor the principle of the separation of powers established in Article 20.2 of the Basic Law are violated. The principle of the separation of powers permits in exceptional cases that legal protection from measures taken by the executive power is not provided by courts of law but by independent institutions appointed or established by Parliament within the functional sphere of the executive power. 122

2. The government of the Free State of Bavaria (a state of the Federal Republic of Germany) regarded the constitutional complaints as unfounded. It was of the opinion that the amendment was urgently required for reasons of credibility in foreign policy as well as for reasons of internal security. The Bavarian government took the position that, raising the thresholds for transfer and use of intelligence so that they are consistent with the concept of *hinreichender Tatverdacht* (reasonable grounds for suspecting a criminal offence), which originates from criminal procedure, is out of the question. According to the government of Bavaria, all laws dealing with the intelligence services part from the assumption that a transfer of information to another security agency or to a prosecuting agency is permissible if there are "*tatsächliche Anhaltspunkte für den Verdacht*" (factual grounds for suspecting) that someone plans, is committing or has committed a specified criminal offence. In many cases, not even this is made a prerequisite for the transfer of information. The regulations about transfer are based on the idea that it is exactly the task of the intelligence services to collect information in the lead-up to a criminal offence to transfer the information to the executive agencies so that they can resist the threat or initiate criminal prosecution. If transfer is also made contingent upon the existence of the same prerequisites that must be fulfilled for investigative activities in the context of the prosecution of criminal offences, this will make the intelligence service a subsidiary organ of the public prosecutor's office, which will in the end, result in the intelligence service becoming a prosecuting agency. The legal hurdle for data transfer must be lower than the interference threshold of the prosecuting agencies. 123

3. The Federal Data Protection Commissioner was of the opinion that strategic surveillance, also under the modified conditions, is consistent with the Basic Law because it does not serve to identify specific persons or subscriber lines. The Federal Data Protection Commissioner suggests, however, that in order to ensure its conformity with the Basic Law it must be interpreted in such a way that the personal data obtained during the monitoring shall not be used for objectives set forth in § 3.3 of the G 10 Act, as had been established as a principle in § 3.2(1) of the G 10 Act (old version). According to the Federal Data Protection Commissioner, the regulation is, in principle, constitutional if this condition is fulfilled, as this condition prescribes procedural arrangements for the prevention of abuse. 124

The Federal Data Protection Commissioner, to the extent that the complainants challenge § 3.2(3) of the G 10 Act, also has considerable reservations concerning the constitutionality of the provision. The Federal Data Protection Commissioner noted that Article 10 of the Basic Law is a human right and that the data obtained abroad is processed on the domestic territory. 125

The regulation set forth in § 3.3(2) of the G 10 Act in conjunction with § 12 of the *Bundesnachrichtendienstgesetz* (BNDG, Federal Intelligence Service Act) is problematic from the point of view of constitutional law, in the view of the Federal Data Protection Commissioner, because the regulation does not sufficiently determine the objectives for which the data may be used. For the Federal Data Protection Commissioner it seemed contradictory that, on the one hand (pursuant to §§ 3.4 and 3.6 of the G 10 Act), personal data is to be checked for its necessity and that it shall be destroyed or deleted if appropriate, while on the other hand, it should be transferred to the Federal government in the framework of the duty to inform pursuant to § 3.3(2) of the G 10 Act in conjunction with § 12 of the BNDG. The Federal Data Protection Commissioner suggested that there is the danger that in practice, the duty to inform will gain priority over the deletion of data which may be necessary. 126

The Federal Data Protection Commissioner also claimed that the restriction of telecommunications privacy by the powers established in § 3.1 sent. 2 nos. 2-6 of the G 10 Act raises concerns regarding the principle of proportionality. 127

Certainly, as can be seen from the legislative process and the associated materials, the powers conferred to the Federal Intelligence Service do not constitute an expansion of its mission. The Federal Data Protection Commissioner argued, rather, that the Federal Intelligence Service is granted the authority to conduct surveillance only to the extent that such surveillance in specific circumstances is consistent with its mission. Monitoring pursuant to § 3.1 of the G 10 Act that is independent of the existence of a suspicion must, however, be aimed at collecting pertinent information and must, in particular, not result in circumventing the threshold for an encroachment upon fundamental rights in the case of monitoring of individuals based on suspicion. Apart from that, the Federal Data Protection Commissioner claimed that an intelligence service investigation which serves police tasks in the lead-up to a criminal of- 128

fence also contradicts the separation of competencies between the police and the secret services established by constitutional law.

In the opinion of the Federal Data Protection Commissioner, the quantitative dimension of the permitted encroachments upon the right to telecommunications privacy makes the justification, which invokes prevailing interests of the common good, also seem doubtful. Apart from that, the actual extent of ordered encroachments upon fundamental rights remains almost undefined from the normative point of view and is, essentially, only subject to limitations on the Federal Intelligence Service's resources and staff. 129

The Federal Data Protection Commissioner argues that for the weighing of the monitored persons' interests, it must certainly be assumed that the participants of an act of communication can be identified. The additional powers for collecting data are, however, not aimed at subsequent encroachments related to specific individuals for the objective of resistance to a threat but are aimed at a pertinent analysis of the situation in order to devise a foreign-policy counter strategy. The restriction of telecommunications privacy required for this analysis has already been correctly described by the Federal Constitutional Court as a "relatively minor burden placed on the individual and, as such, a low-intensity encroachment upon a fundamental right". The Federal Data Protection Commissioner concludes that the awareness of such a use taking place, which is anonymous in its objective, will hardly result in uncertainties in the exercise of fundamental rights. 130

Under the aspect of the general interest which is to be weighed against this, the Federal Data Protection Commissioner noted that it is important that the respective powers are vested in the Federal Intelligence Service only in the framework of its mission. In accordance with the definition of its mission, it is not sufficient that individual legal interests in the field of internal security are jeopardised because the matter in question must constitute a serious threat to the security or the existence of the Federal Republic of Germany in its entirety. The grounds which justify the forecast that a danger threatens the state must be put forward and substantiated in the reasoning of the application, and they are subject to an examination by the responsible Federal minister, by the parliamentary panel and by the commission established pursuant to § 9 of the G 10 Act. 131

The Federal Data Protection Commissioner took the position that § 3.4 of the G 10 Act is constitutional, provided that it does not allow a targeted evaluation for the objectives of secondary use permitted by § 3.3 of the G 10 Act. 132

The Federal Data Protection Commissioner took the position that § 3.5 in conjunction with § 3.3 of the G 10 Act violates the principle of proportionality to the extent that the power to change the objective set forth in § 3.3 of the G 10 Act leads to the result that investigations that are carried out independently of the existence of a suspicion, by means of collecting "incidental information" in a targeted way, indirectly circumvent the suspicion-related criminal offence element prerequisites that are required for indi- 133

vidual monitoring in accordance with the principle of proportionality. The legal regulation according to which "*tatsächliche Anhaltspunkte*" (factual grounds), *i.e.* intelligence collected in the lead-up to a criminal offence below the threshold of the criminal-law standard of an initial suspicion, are already sufficient, permits a change of objective in the case of all intelligence which contains, albeit remote, indications towards the specified elements of a criminal offence, thus permitting the impermissible collecting of data that can serve as the factual basis for individual proceedings.

134 The Federal Data Protection Commissioner concluded that, unlike in the case of the original strategic surveillance regulation, the collecting of data is now aimed at gaining intelligence which is also of interest for the secondary objectives. In this type of encroachment, which consists of the obtaining of intelligence and which has a double relevance from the outset, the result of any authorisation to change the objective which would permit the secondary use of any relevant intelligence is that an investigation that is independent of the existence of a suspicion factually takes place for the secondary objective as well. If in the case of an encroachment that has a double relevance, too many subjects of monitoring are affected by the secondary use of the intelligence obtained, the provision that regulates the change of objective must, as a legal interface, assume a compensatory filtering function. In the opinion of the Federal Data Protection Commissioner, in this context a secondary use can only be permissible to the extent that the suspicion becomes more concrete in a way that goes considerably beyond the initial suspicion and that ensures in a sufficient way that the number of factually uninvolved persons who become targets of measures by the security agencies is not disproportionately large.

135 The Federal Data Protection Commissioner argued that the transfer of intelligence obtained in the lead-up to a criminal offence by means of investigations that have a double relevance undermines the separation between the Federal Intelligence Service and "police agencies" to such an extent that it is reduced to a mere formality. In this respect, § 3.5 of the G 10 Act also violates the principle of separation between the secret services and the police. For co-operation to take place between the Federal Intelligence Service and “police agencies” in accordance with the Constitution, a filter that takes the form of a higher threshold of suspicion is required. If agencies that receive collected information hold police powers and are therefore, for reasons of the rule of law, not authorised to conduct lead-up investigations with intelligence service means, this threshold is even higher than in the case of the Federal Intelligence Service co-operating with the other intelligence services.

136 The Federal Data Protection Commissioner asserted that, in consideration of the special need for protection and the special risks posed by the threats at issue in the G 10 Act, a filter between primary and secondary objective is required that provides especially effective organisational safeguards. By means of § 3.5(2) of the G 10 Act, the parliament has established procedural arrangements which reserve the decision to an official who is qualified to hold judicial office. This provision serves to take an informed decision but does not assure that the interests of the subject of monitoring are

also independently taken into consideration by an institution that is not bound by instructions from agencies concerned with, and that is not involved in, security policy interests. Procedural arrangements that make it possible for the institution charged with the responsibility of controlling data protection to effectively control, at least subsequently, the decision to change the objective of monitoring, which is of special importance, at a minimum require that a record is kept of the decision and that organisational measures are taken which facilitate targeted access to this evidence.

According to the Federal Data Protection Commissioner, the restriction of information set forth in § 3.8(2) of the G 10 Act is consistent with the Basic Law only to the extent that it does not impair the monitored person's possibilities for legal protection provided by the right of recourse to a court. This is the case only if a need for legal protection is already precluded for abstract considerations. At most, this is the case if the collection and the use of data occurs without any reference whatsoever to the person being monitored. This threshold is passed in any case if the Federal Intelligence Service stores the data by means of technical equipment in such a way that evaluation that is related to individuals is possible or if it transfers them to the security agencies specified in § 3.5 of the G 10 Act in a manner that establishes a direct relation to those being monitored. To the extent that the data has been used in a manner that is directly related to the subject of the monitoring, notification must take place. The Federal Data Protection Commissioner concluded that in this respect, § 3.8(2) of the G 10 Act is unconstitutional. 137

As concerns the fact that recourse to a court is, pursuant to § 9.6 of the G 10 Act, precluded in the case of strategic telecommunications monitoring, the Federal Data Protection Commissioner argues that the guaranteed recourse to a court established by Article 19.4 of the Basic Law is not subject to a legal regulation. However, strategic telecommunications surveillance, when interpreted in conformity with the Constitution, is not aimed at specific individuals in spite of the fact that the technical possibility of establishing references to individuals has increased considerably. Recourse to a court, pursuant to § 5.5(3) of the G 10 Act must be possible in the event that, contrary to the originally determined objective, a reference to individuals has been established as an incidental result. 138

4. A majority of the data protection commissioners of the *Länder* (states) who gave their opinions on the constitutional complaints expressed constitutional reservations, albeit with different focuses, as regards the challenged regulations. Only the Bavarian Data Protection Commissioner considered the Act to be consistent with the Basic Law when interpreted in conformity with the Constitution. Nevertheless, the Bavarian Data Protection Commissioner argued that an initial suspicion is not a sufficient reason for the transfer of personal data pursuant to § 3.5 of the G 10 Act. Only in the case of the existence of qualified grounds for suspicion may data be transferred to other agencies. Apart from that, seamless control must be ensured. To achieve this, the powers of the commission and of the data protection commissioners must be determined in a precise way and must be co-ordinated. 139

In their opinions, the other data protection commissioners criticised, *inter alia*, that the Act has expanded the Federal Intelligence Service's mission in an unconstitutional manner. They argued that the law involves the Federal Intelligence Service in tasks concerned with crime prevention and prosecution, thus employing it for internal security objectives. This violates the principle of separation between the secret services and the police. In view of the imbalance between efforts and return and in view of the possibility of effectively encrypting telecommunications contacts, it is doubtful whether the powers that the Act confers to the Federal Intelligence Service are suitable and required. Nor are the powers of encroachment upon fundamental rights proportional in the strict sense of the word. On the one hand, the threatening situations that justify monitoring measures which have been newly incorporated into the Act carry far less weight than the threat of an armed aggression. On the other hand, the restrictions of fundamental rights in this context are considerable from the quantitative as well as from the qualitative point of view. The permission to screen foreign subscriber lines in a targeted manner goes beyond what is permissible from the constitutional point of view. 140

The data protection commissioners of the *Länder*, with the exception of the Bavarian Data Protection Commissioner, argued that the challenged regulations also do not determine the objectives for which the personal data obtained by means of telecommunications monitoring may be used; in particular, the regulations do not bind the use of the data strictly enough to specified objectives. The level of suspicion which justifies the transfer of the data to other agencies is too low. There are better ways for protecting the anonymity of the subjects of monitoring. Almost all of the opinions presented cast doubts on the Act’s preclusion or limitation of the duty to inform, some also express reservations about precluding the recourse to a court. All the data protection commissioners regarded their possibilities for control as insufficient. 141

IV.

At the oral argument, opinions were given by: the complainants, the Federal government, the Federal Intelligence Service, the Federal Data Protection Commissioner, the data protection commissioners of the *Länder* (states) Berlin and Hamburg, the G 10 parliamentary panel, the G 10 Commission, and by the independent, court-appointed experts Professor Dr. Pfitzmann, Professor Dr. Waibel and Professor Dr. Wiesbeck. 142

B.

With the exception of the constitutional complaint lodged by the second of the two complainants bringing the second constitutional complaint (1 BvR 2420/95), the constitutional complaints are admissible. 143

I.

Only someone who is personally, presently and directly affected by the challenged 144

regulations may lodge a constitutional complaint against the law that establishes those regulations (cf. BVerfGE 90, p. 128 [at p. 135]; established case-law). If a complainant is affected in his or her fundamental rights only by the application of the challenged law, constitutional complaints may not be lodged against the law itself, but must be lodged against the act of enforcing the law. There is, however, no possibility of challenging the enforcement of a law if the person affected cannot obtain knowledge of such enforcement. In these cases, the person must be entitled to directly lodge a constitutional complaint against the law just as he or she would be entitled to do in those cases in which fundamental rights are affected by the law itself, *i.e.* without any act of enforcement (cf. BVerfGE 30, p. 1 [at pp. 16-17]). Under these circumstances, the requirements placed on the justification of the constitutional complaint pursuant to Article 23.1(2) and Article 92 of the *Bundesverfassungsgerichtsgesetz* (BVerfGG, Federal Constitutional Court Act) are fulfilled if the complainant demonstrates that there is some probability that his or her fundamental rights are being affected by measures taken pursuant to the challenged statutes (cf. BVerfGE 67, p. 157 [at p. 170]).

II.

The majority of the constitutional complaints in the present proceedings comply with these prerequisites. 145

1. Normally, the complainants cannot obtain knowledge of possible measures taken pursuant to § 1.1 and § 3 of the G 10 Act, which would affect them. 146

Certainly, the regulations at issue in this case do not independently impose themselves on the complainants. Rather, ministerial provisions and orders, including monitoring, recording, evaluation and transfer by the Federal Intelligence Service (and, if necessary, measures of reception, examination and use by the agencies to whom the Federal Intelligence Service must supply data) must occur in order for the legal regulations to become effective. Only these measures constitute a specific impairment of the respective holders of fundamental rights. 147

These steps of implementation, however, take place unnoticed by the persons affected and are imperceptible for them. In the interest of promoting their very objective, the implementation of the Act and its regulations is largely kept secret. The law only provides that the person who has been subject to monitoring activities be informed after the fact and in compliance with the terms and limitations set forth in § 3.8 of the G 10 Act. Due to the restrictions set forth therein, the subjects of monitoring rarely learn that they have been monitored and whether personal data obtained from the monitoring was evaluated, transferred and submitted for further use. 148

2. The complainant bringing the first constitutional complaint, the first of the two complainants bringing the second constitutional complaint, and both complainants bringing the third constitutional complaint have sufficiently established that it is possible that their fundamental rights are being violated. 149

a) The complainant bringing the first constitutional complaint is a university lecturer, who, according to his own statement, works in the area of criminal law in the field of narcotics and who, in connection with his work, maintains numerous contacts abroad which take place, *inter alia*, per telephone and per fax. As, pursuant to § 3.1 sent. 2 no. 4 of the G 10 Act, the introduction of narcotics from abroad into the Federal Republic of Germany is one of the areas in which the Federal Intelligence Service obtains intelligence by monitoring telecommunications traffic, it is also possible that the complainant's telecommunications traffic is screened and recorded and that its content is taken note of. If the screened telecommunications traffic contains one of the search concepts, a relevance check is performed and it is possible that the telecommunications traffic is used by the Federal Intelligence Service. In view of the broad scope of the constituent elements of a criminal offence set forth in § 3.5 of the G 10 Act, it cannot be excluded that the recorded telecommunications traffic is transferred to other agencies triggering further examination by these agencies. 150

b) The first of the two complainants bringing the second constitutional complaint (2a) is a German citizen with her permanent residence in Uruguay. In her statement, she claims that she works as a free-lance journalist for German and foreign newspapers, radio and television stations especially on the topics that are subject to monitoring by the Federal Intelligence Service. This statement is also sufficient for substantiating that her fundamental rights are being affected because, for the following two reasons, her statement cannot be more specific: (1) telecommunications monitoring takes place without any actual suspicion and is kept secret, and (2) the measures that follow monitoring are also beyond the complainant's knowledge. 151

The fact that the complainant does not live in Germany does not preclude the possibility that her fundamental rights are being affected. The complainant's telecommunications traffic can be covered by the monitoring measures, as the monitoring measures are targeted especially to international telecommunications links. Therefore, the complainant's fundamental rights can be violated even if her permanent residence is abroad. 152

To the extent that the complainant extends her challenge to § 1.1, § 3.1(1) and § 3.1 sent. 2 no. 1 of the G 10 Act, the challenge is admissible because the one-year time limit set forth in § 93.3 of the Federal Constitutional Court Act has not lapsed. Certainly, the regulations have not been amended by the 1994 Fight against Crime Act. However, the Fight against Crime Act, in particular the provisions on the powers to use and transfer data set forth in § 3.3 and § 3.5 of the G 10 Act (new version), have embedded the regulations in a new legal environment so that the implementation of the older regulations can now have a new negative impact. Pursuant to the established case-law of the Federal Constitutional Court, this tolls the one-year time limit, before the running of which constitutional complaints against statutes are still admissible (cf. BVerfGE 45, p. 108 [at p. 119]; 78, p. 350 [at p. 356]). 153

c) The first of the two complainants bringing the third constitutional complaint (3a) is 154

a newspaper publisher. Pursuant to Article 19.3 of the Basic Law, the complainant, as a legal person, is also entitled to the protection of Article 10 of the Basic Law. According to the complainant's statement, reports on the subjects of corruption, international terrorism, international trade in drugs and arms, money laundering, organised crime, intelligence service activities, and plutonium smuggling are among the editorial focuses of its newspaper. The complainant maintains correspondents' posts in other countries and co-operates, *inter alia*, with the second complainant (3b) and other German and foreign correspondents, journalists and publishers outside Germany. The mentioned topics are subjects of the Federal Intelligence Service's telecommunications monitoring. Complainant (3a), to this extent, is similarly situated along with the complainant bringing the first constitutional complaint. The statement made by complainant (3a) also shows that it is not a remote assumption that the Federal Intelligence Service may take note of the complainant's editorial projects, a likelihood that impairs the complainant's procurement of information.

d) The second of the two complainants bringing the third constitutional complaint (3b) is a journalist with permanent residences in Germany and Italy. In his statement, he argues that he researches and publishes, *inter alia*, in the areas of international terrorism, international trade in drugs and arms, money laundering, organised crime and intelligence service activities, and that he, in this context, maintains many contacts at home and abroad. As in the case of the first complainant bringing the third constitutional complaint, this is sufficient to justify a possible impact on his fundamental rights. 155

3. Contrary to the circumstances of the other complainants, the second of the two complainants bringing the second constitutional complaint has not sufficiently established that he is personally and directly affected by the legal regulations that he challenges. He is an Uruguayan citizen with his permanent residence in Uruguay. In his statement, he claims that that he takes care of the telecommunications traffic of the first of the two complainants bringing the second constitutional complaint when she is absent. As he does not provide any further details, his statement does not show, to the required degree of probability, that his fundamental rights are affected by measures taken pursuant to the challenged regulations. 156

C.

The challenged regulations are not fully consistent with the Basic Law. 157

I.

The standard applied to the review of the constitutionality of the challenged legislation is, above all, Article 10 of the Basic Law. Article 10 of the Basic Law protects interests that are distinct from the right to informational self-determination that follows from Article 2.1 in conjunction with Article 1.1 of the Basic Law. As concerns telecommunications traffic, Article 10 of the Basic Law contains a special guarantee which supersedes the general protections of Article 2.1 (cf. BVerfGE 67, p. 157 [at p. 171]). To 158

the extent that the possibility of taking recourse to a court against measures taken pursuant to § 3 of the G 10 Act is concerned, Article 19.4 of the Basic Law is relevant as well. The same is true regarding the restrictions on the recourse to a court set forth in § 9.6 of the G 10 Act. Apart from that, the constitutional complaints lodged by the first of the two complainants bringing the second constitutional complaint and both complainants bringing the third constitutional complaint are to be reviewed in accordance with the standards established in Article 5.1(2) of the Basic Law.

1. Article 10 of the Basic Law protects telecommunications privacy. 159

a) Telecommunications privacy covers, first and foremost, the content of an act of communication. Public authority is, in principle, not supposed to have the possibility of obtaining knowledge about the content of the exchange of information and thoughts, whether oral or written, that takes place via telecommunications equipment. In this context, Article 10 of the Basic Law draws no distinction between communication of a private nature and other communication, *e.g.* business or political communication (cf. BVerfGE 67, p. 157 [at p. 172]). To the contrary, the protection of fundamental rights extends to all acts of communication that take place by means of telecommunications technology. 160

The protection of fundamental rights, however, is not restricted to shielding the content of an act of communication against the state taking note of it. The protection of fundamental rights also covers the circumstances of communication, particularly including: (1) information about whether, when and how often telecommunications traffic has taken place or has been attempted; (2) information about the individuals between whom telecommunications traffic has taken place or has been attempted; and (3) information about which subscriber lines have been used (cf. BVerfGE 67, p. 157 [at p. 172]; BVerfGE 85, p. 386 [at p. 396]). The state cannot, in principle, claim to be allowed to take note of the circumstances of acts of communication. The use of the medium of communication is supposed to remain confidential in all respects. 161

By withdrawing, in principle, individual acts of communication from the state's access, the fundamental right protecting telecommunications privacy intends to preserve the conditions of free telecommunication in general. The inviolability of telecommunications privacy, as a fundamental right, seeks to avoid the following: that the exchange of opinions and information by means of telecommunications equipment ceases altogether or is modified in its form and content because communication partners expect the state: (1) to interfere with their communication; or (2) to take note of the circumstances or the content of their communication. 162

Apart from that, the freedom of the use of telecommunications that is safeguarded by Article 10 of the Basic Law suffers if there is fear that the state utilises knowledge about the circumstances and the contents of acts of telecommunication in other contexts to the detriment of the telecommunications partners (cf., altogether, BVerfGE 65, p. 1 [at pp. 42-43]; BVerfGE 93, p. 181 [at p. 188]). For these reasons, the protection provided by Article 10 of the Basic Law extends not only to the state taking note 163

of acts of telecommunication that the telecommunications partners wish to keep to themselves, but also to the procedures by which information and data are processed that follow the state's taking note of protected acts of communication and the use of the knowledge obtained therefrom (concerning the right to informational self-determination, cf. BVerfGE 65, p. 1 [at p. 46] already).

b) Certainly, Article 10.2 of the Basic Law permits restrictions of telecommunications privacy. Such restrictions, however, require, as does every restriction of a fundamental right, a legal regulation that serves a legitimate aim in the public interest and respects the principle of proportionality. Article 10 of the Basic Law also places special requirements on the parliament that particularly refer to the processing of personal data that has been obtained through interference with telecommunications privacy. The standards the Federal Constitutional Court developed for the right to informational self determination pursuant to Article 2.1 in conjunction with Article 1.1 of the Basic Law, in its "Census" decision (cf. BVerfGE 65, p. 1 [at pp. 44 *et seq.*]), can largely be applied to the more specific guarantee in Article 10 of the Basic Law. 164

One of these standards is that the prerequisites for and the extent to which privacy may be restricted must be clearly recognisable by an objective person in the regulations. In particular, the objective for which telecommunications privacy may be restricted must be precisely specified, naming the area of threat to which it refers. The data collected must also be suitable and necessary for achieving the objective of the restriction on telecommunications privacy. It would be incompatible with this principle to create, for unspecified objectives or for objectives that cannot yet be specified, a stock of data, the sources of which are not anonymous. Therefore, the storage and the use of collected data is, in principle, bound to the objective specified in the law that empowers the respective agency to take note of the collected data in the first place. 165

Acts of communication do not lose their Article 10 privacy protection because the state has been able to learn of the existence of the telecommunications contact; the standards established pursuant to fundamental rights apply equally to the transfer of data and information that has been obtained by an infringement of telecommunications privacy. The protections apply all the more, as the transfer of data, as a general rule, does not only result in an increase of the agencies or persons who are informed about the act of communication but also leads to the fact that the data is conveyed to a different context for altogether new uses. This after-effect of the transfer of data involves additional, possibly more serious, consequences for the monitored persons than when registered only in its original context of use. 166

Certainly, the principle of tying an encroachment on telecommunications privacy to a specific objective does not altogether preclude the possibility that the objective for such an encroachment might change. Any changes, however, require a statutory basis consistent in form and substance with the Basic Law. This means, *inter alia*, that a change of the objectives that justify encroachments upon privacy must be justified by 167

interests of the common good that rise above the interests that are protected by the Basic Law. The new intended use of the data must refer to the missions and authorities of the agency to which the data is transferred, and its wording must respect the principle of clarity. Moreover, the objective for which the data was originally collected must not contradict the new objective being offered as the justification for the collection or use of the data (cf. BVerfGE 65, p. 1 [at pp. 51, 62]).

168 Assurance that the rule, which requires that all encroachments upon telecommunications privacy must be bound to a specific objective, is observed, can only be had if, after the data has been screened, it can still be determined whether the data was collected by means of an encroachment upon telecommunications privacy. Therefore, constitutional law requires that the data be marked accordingly.

169 Moreover, Article 10 of the Basic Law stipulates that the holders of fundamental rights are entitled to be informed of telecommunications monitoring that involved them. This requirement ensures the effective protection of fundamental rights, as without such notification, the monitored persons can neither claim that the screening and monitoring of their telecommunications contacts were illegal, nor can they assert possible rights regarding deletion or correction with respect to the collected data. Such a claim is not, from the outset, restricted to the recourse to a court that follows from Article 19.4 of the Basic Law. First of all, it is rather a specific right to data protection that can be asserted *vis-à-vis* the state agency that processes information and data.

170 The Basic Law does not prescribe in detail the manner in which the monitored person is to be informed. The Constitution only requires that the people being monitored be notified in those cases where the data was collected secretly and the monitored persons were not entitled to demand that they be informed of the monitoring, or if the notification to which the monitored persons were entitled did not adequately take their rights into account (cf. BVerfGE 30, p. 1 [at pp. 21, 31-32]). The duty to inform, however, is also subject to the reservation of Article 10.2 of the Basic Law. To the extent that the encroachment upon telecommunications privacy cannot achieve its aim if the monitored person is informed of the monitoring activity, it is not objectionable from the constitutional point of view to restrict the notification that monitoring is taking place accordingly. It may be sufficient to inform the monitored person about the encroachment after the fact (cf. BVerfGE 49, p. 329 [at pp. 342-343]).

171 An encroachment upon telecommunications privacy can be imperceptible and the subsequent act of processing the obtained data is unfathomable for the unsuspecting subject of telecommunications monitoring; moreover, the possibility of restricting notification about an encroachment leads to gaps in legal protection. For these reasons, Article 10 of the Basic Law requires that controls be incumbent on state agencies and subsidiary agencies that are independent and not bound by instructions (cf. BVerfGE 30, p. 1 [at pp. 23-24, pp. 30-31]; BVerfGE 65, p. 1 [at p. 46]; BVerfGE 67, p. 157 [at p. 185]). The Constitution, however, does not prescribe how these controls are to be

organised. The parliament is free to choose the manner it regards as the most suitable, always provided that it adequately takes into consideration fundamental rights. One aspect of adequacy is that the controls cover each step of the process of telecommunications monitoring. The legitimacy of an encroachment upon telecommunications privacy, as well as the compliance with the legal regulations for the protection of telecommunications privacy, must be controlled.

Finally, as the screening and recording of telecommunications traffic and the use of the information thus obtained is bound to specific objectives, the obtained data must be destroyed as soon as it is no longer required for the specified objectives or for legal protection by recourse to a court. 172

c) Constitutional jurisprudence has not yet clarified how far the geographical range of the protection provided by Article 10 of the Basic Law extends. The Federal government assumes, though it remains an open question, that the constitutional protection of Article 10 only applies if there is a sufficiently close relationship to the territory of the Federal Republic of Germany. This interpretation leads to the conclusion that the Article 10 protection neither extend to foreign telecommunications traffic nor to persons living abroad. This question has not arisen in this way before because state power, as a general rule, could only be exercised on the territory of the state. Generally, the borders of the state were at the same time the borders of state power. Only the development of technology has made it possible for the state to extend its activities to the territory of other states without having to be physically present there in the shape of representative entities. In particular, the use of satellites permits, *inter alia*, the monitoring of acts of communication conducted outside Germany without a physical connection to that foreign territory. 173

The starting point of the answer to the question about the territorial scope of Article 10 of the Basic Law is Article 1.3 of the Basic Law, which determines the scope of the application of the fundamental rights in general. The fact that this regulation provides that the fundamental rights bind the legislature, the executive and the judiciary in a comprehensive way, does not, however, result in a final determination of the territorial scope of application of the fundamental rights. The Basic Law does not content itself with defining the internal order of the German state but also determines the essential features of the German state's relationship to the community of states. In this respect, the Basic Law assumes that a delimitation between states and legal systems is necessary, and that co-ordination between states and legal systems is also necessary. On the one hand, the scope of competence and responsibility of organs of the German state must be taken into account when determining the scope of application of the fundamental rights (cf. BVerfGE 66, p. 39 [at pp. 57 *et seq*.]; BVerfGE 92, p. 26 [at p. 47]). On the other hand, constitutional law must be co-ordinated with international law. International law, however, does not, in principle, preclude the validity of fundamental rights in matters that bear on relations with foreign countries. The territorial scope of the fundamental rights, however, must be drawn from the Basic Law itself, taking into account Article 25 of the Basic Law. When doing so, modification and 174

differentiation may be permissible or required, depending on the relevant rules of constitutional law (cf. BVerfGE 31, p. 58 [at pp. 72 *et seq*.]; BVerfGE 92, p. 26 [at pp. 41-42]).

175 The protection of telecommunications privacy provided by Article 10 of the Basic Law, in accordance with the provisions of international law (cf. Article 12 of the Universal Declaration of Human Rights of 10 December 1948; Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950; in this context, cf. EGMR [*Entscheidungen des Europäischen Gerichtshofs für Menschenrechte*, Decisions of the European Court of Human Rights], NJW [*Neue Juristische Wochenschrift*] 1979, p. 1755 [at p. 1756]), aims at assuring that telecommunications remain free of undesired or unnoticed monitoring and that the holders of fundamental rights can communicate in an unhindered way. The protection of telecommunications privacy relates to the medium of communication itself and intends to counteract the threats to confidentiality that result precisely from the use of this medium, which is more likely to be the object of encroachment by the state than direct communication between partners who are physically present (cf. BVerfGE 85, p. 386 [at p. 396]. Modern technology, like satellite and microwave technology, permits access to foreign telecommunications traffic by means of monitoring equipment that is located on the territory of the Federal Republic of Germany.

176 The screening and recording of telecommunications traffic with the help of the Federal Intelligence Service's reception equipment located on German soil already establishes a technical and informational relation to the respective participants in an act of communication and, depending on the particular characteristics of data and information, establishes a contact to a specific territory. The evaluation, by the Federal Intelligence Service, of the acts of telecommunication that were screened in this way takes place on German soil. Under these circumstances, an act of communication abroad is linked with the action of the state on the domestic territory in such a way that the fundamental rights pursuant to Article 10 of the Basic Law are binding even if it must be supposed, for this binding effect to apply, that the territorial reference must be sufficiently close. Secret service activities that do not fall under the G 10 Act are not to be decided in this context, nor is the question of the legal situation of foreign communication partners abroad. In any event, pursuant to Article 19.3 of the Basic Law, Article 10 of the Basic Law does not apply to foreign legal entities.

177 2. Parts of the challenged regulations are also to be reviewed applying the standards of Article 19.4 of the Basic Law.

178 Article 19.4 of the Basic Law establishes the citizen's right to effective judicial review in cases in which it seems possible that their rights have been violated by acts of state power (by the German authorities). In Article 10.2(2) of, however, the Basic Law makes an exception to this guarantee exclusively with respect to encroachments upon telecommunications privacy. Pursuant to Article 19.4(3) of the Basic Law, this exception is unaffected by the otherwise comprehensive guarantee of legal protection

provided by the guarantee of recourse to a court. These provisions, however, do not set forth that the encroachments are not subject to any review whatsoever. Rather, recourse to a court is replaced by a review of the case by agencies and auxiliary agencies appointed by the parliament.

The right provided by Article 19.4 of the Basic Law, however, is not restricted to judicial review and judicial proceedings. If the guarantee of legal protection provided by the right of recourse to a court is supposed to ensure the possibility of safeguarding other material rights, this guarantee can, parallel to Article 10 of the Basic Law, require that a monitored person be informed of the monitoring activities, if this form of granting knowledge is the prerequisite of the monitored person taking recourse to a court (cf. BVerfGE 65, p. 1 [at p. 70]). However, Article 19.4 of the Basic Law, which must be made more concrete and implemented by laws, does not preclude limitations on the right that it secures. 179

The obligation to destroy data that is no longer needed, which exists in principle, must also be understood in light of Article 19.4 of the Basic Law. The guaranteed right of recourse to a court provided by Article 19.4 of the Basic Law prohibits measures that are aimed at and likely to frustrate the protection of the monitored person's right of recourse to a court (cf. BVerfGE 69, p. 1 [at p. 49]). In cases in which the monitored person strives for judicial review of state measures of information and data processing, the obligation to destroy data must therefore be reconciled with the guarantee of recourse to a court in such a way that legal protection is not undermined or frustrated. 180

3. The fundamentally private acts of communication protected by Article 10 of the Basic Law, including correspondence, post and telecommunication, can be further protected by guarantees of fundamental rights that are relevant because of the content or the context of a specific act of communication. Guarantees of protection in addition to Article 10 may also be necessary in light of the impairment of fundamental rights that might result from use of the obtained data in new contexts. 181

To the extent that the complainants engage in the press sector and to the extent that they have claimed that they are hindered in this activity by the challenged regulations, the freedom of the press pursuant to Article 5.1(2) of the Basic Law can be considered as an additional guarantee of a fundamental right to telecommunications privacy. The freedom of the press not only refers to the dissemination of news and opinions in the press but also includes the prerequisites and auxiliary activities without which the press is unable to fulfil its function. This especially applies to the secrecy of its sources of information and to the mutual trust between the press and its informants (cf. BVerfGE 20, p. 162 [at pp. 176, 187 *et seq.*]; BVerfGE 50, p. 234 [at p. 240]; BVerfGE 77, p. 65 [at pp. 74-75]) as well as to the confidentiality of editorial work (cf. BVerfGE 66, p. 116 [at pp. 130 *et seq.*]), all of which are imperative for the procurement and the processing of information. 182

This protection, however, can only apply after the state has taken note of data and 183

information that was obtained by way of telecommunications monitoring. Due to the fact that screening is untargeted, it is not possible for the Federal Intelligence Service to ascertain, before it has taken note of an act of communication, that the communication is related to the press, which also means that the Federal Intelligence Service lacks the possibility to respect the protective effects of the freedom of the press before taking note of an act of communication. This fundamental right, however, must be taken into account when recording, using and transferring data and information.

II.

The challenged regulations allow encroachments upon the aforementioned fundamental rights in several respects. 184

1. The monitoring and recording of acts of wireless international telecommunication by the Federal Intelligence Service encroaches upon telecommunications privacy. 185

As Article 10.1 of the Basic Law intends to protect the confidentiality of communication, every effort to take note of, record and utilise communication data by the state is an encroachment upon fundamental rights (cf. BVerfGE 85, p. 386 [at p. 398]). There is, therefore, no doubt that the fact that Federal Intelligence Service staff takes note of screened acts of telecommunication constitutes an encroachment upon fundamental rights. In order to determine whether this also applies to the measures that precede analysis by the Federal Intelligence Service, they must be regarded in their context that is determined by the objective of monitoring and of the use of the obtained data. 186

This means that the screening alone constitutes an encroachment, to the extent that it makes the communication available to the Federal Intelligence Service and is the basis of the subsequent comparison with the search concepts. Screening does not constitute an encroachment to the extent that acts of telecommunication between German subscriber lines were also screened in an untargeted manner and solely for technical reasons but were discarded by technical means immediately after signal editing without leaving any indication that monitoring had taken place. The mere fact that the obtained data cannot be immediately attributed to specific persons does not mean that there has been no encroachment; it was confirmed at the oral argument that in these cases it is also possible, without any difficulty, to establish references, especially to the identity of individuals. 187

The encroachment upon telecommunications privacy persists through the storage of the screened data, which makes the material available for comparison with the search concepts. The comparison itself constitutes an encroachment, as it comprises the selection of data for further evaluation. This applies whether or not the comparison takes place automatically or is carried out by staff of the Federal Intelligence service who, for this objective, takes note of the content of the act of communication. As the further storage after screening and comparison serves to make the data available for evaluation, it is also an encroachment upon Article 10 of the Basic Law. 188

The examination made pursuant to § 3.4 of the G 10 Act, which determines whether the personal data obtained by telecommunications monitoring is required for the objectives which justify these measures, also constitutes an encroachment. This examination is an act of selection by which the recorded data is either submitted to further use, stored for further use or destroyed. 189

An encroachment upon the right to telecommunications privacy also occurs when the Federal Intelligence Service, in the framework of its duty to inform the Federal government, transfers personal data that it has obtained through telecommunications monitoring. This transfer of the collected data expands the circle of those who know of the acts of communication and can make use of this knowledge. The Federal Intelligence Service's transfer of this recorded data to the receiving agencies, an act that is regulated in § 3.5 and § 3.3 of the G 10 Act, constitutes an encroachment upon telecommunication privacy, as does the further examination by the receiving agencies, which is regulated in § 3.7 of the G 10 Act. 190

The limitation imposed by § 3.8(1) and § 3.8(2) of the G 10 Act on the duty to inform the monitored person about the monitoring taking place also constitutes an encroachment upon the fundamental right to telecommunications privacy. 191

2. Moreover, the guarantee of the right of recourse to a court provided by Article 19.4 of the Basic Law is impaired by: (1) the limitation, contained in § 3.8(1) and § 3.8(2) of the G 10 Act, on the duty to inform the monitored person that monitoring has taken place; and (2) the preclusion of the recourse to a court contained in § 9.6 of the G 10 Act. Apart from that, the obligation to destroy personal data pursuant to §§ 3.6, 3.7 and 7.4 of the G 10 Act can have a detrimental effect on the judicial review of the measures. 192

3. To the extent that measures ordered on the basis of §§ 1.1 and 3.1 of the G 10 Act also cover telecommunications links of press publishers or journalists, an impairment of the fundamental right of the freedom of the press also occurs as a result of: (1) the authority to examine such acts of telecommunication that is conferred upon the Federal Intelligence Service pursuant to § 3.4 of the G 10 Act; (2) the duty to inform the Federal government; (3) the authority to transfer data to other agencies pursuant to §§ 3.5 and 3.3 of the G 10 Act; and (4) the authority to examine the received data conferred upon these agencies pursuant to § 3.7 of the G 10 Act. 193

III.

The authority to monitor and record telecommunications traffic pursuant to § 1.1 and § 3.1 sent. 2 nos. 1-6 of the G 10 Act is, essentially, in accord with Article 10 of the Basic Law. § 3.1 sent. 2 no. 5 of the G 10 Act is not, however, consistent with this fundamental right to the extent that this provision permits monitoring in order to gather intelligence that is necessary to be able to timely recognise counterfeiting committed abroad and to counteract such a threat. 194

1. In the formal sense, there are no problematic constitutional considerations as against the provisions found in § 1.1 and § 3.1 of the G 10 Act. The legislative competence for the matters regulated by these provisions belongs to the Federal Republic of Germany. The Federal Republic's competence follows from Article 73 no. 1 of the Basic Law, which exclusively confers legislation in foreign affairs and defence to the Federal Republic of Germany. 195

a) The concept of foreign affairs addressed Article 73 no. 1 of the Basic Law can only be defined taking the overall division of legislative competencies between the Federal Republic and the *Länder* into consideration. On the one hand, the concept of foreign affairs must not be interpreted in a way that undermines the division of authority between the Federal Republic and the *Länder.* On the other hand, the concept of foreign affairs must be integrated into the exclusive attribution of various competencies to the Federal Republic. Both perspectives exclude a comprehensive understanding of the concept of foreign affairs that encompasses all matters that touch upon relations with foreign countries. Otherwise, neither the dividing line between the distinct authority of the Federal Republic and the *Länder* could be maintained, nor would the Federal competencies, which are mentioned *e.g.* in Article 73 nos. 3, 5 and 10 or in of Article 74.1 no. 4 of the Basic Law (which also deal with matters that bear on relations with foreign countries) make any sense. 196

The attribution of authority in Article 73 no. 1 of the Basic Law must be seen, rather, in the context of relations with foreign states, which shall, pursuant to Article 32.1 of the Basic Law, be conducted by the Federal Republic. According to this interpretation, foreign affairs in the meaning of Article 73 no. 1 of the Basic Law are the issues that are of importance for the relationship of the Federal Republic of Germany to other states or to intergovernmental institutions, especially as regards the organisation of foreign policy. The Federal Constitutional Court's holding, that only affairs that result from the position of the Federal Republic of Germany as an international actor *vis-à-vis* other states may be regarded as foreign affairs, must also be understood along these lines (cf. BVerfGE 33, p. 52 [at p. 60]). 197

This definition does not restrict the concept of foreign affairs to contacts under international law. The definition does not take matters that are regulated under international law, but the German state and its external relations as a starting point. For the German state's external relations, events abroad whose authors are not foreign states themselves may also be of importance. Such events should not, by means of this definition, be excluded from the area of foreign affairs. It is therefore undisputed that the creation of an agency concerned with comprehensive surveillance as regards foreign countries falls under the competence of Article 73 no. 1 of the Basic Law. In contrast, the aforementioned decision only aims at differentiating between the concept of foreign affairs and reactions on the domestic territory to cross-border activities of private individuals (in this case, a law that prohibits the introduction of films that are hostile to the Constitution from abroad into the Federal Republic of Germany); for this reason, the prohibition was not based on Article 73 no. 1, but on Article 73 no. 5 of the 198

Basic Law.

The Federal Republic of Germany is not prohibited from drawing legislative consequences relating to domestic affairs from intelligence about foreign countries that is gathered by making use of its authority under Article 73 no. 1 of the Basic Law, to the extent that the Federal Republic has a competence of its own for issuing such legislation. In the areas touching upon the fight against crime, however, it is of importance that Article 73 no. 10 of the Basic Law confers to the Federal Republic of Germany specified and, at the same time, limited legislative authority concerning the co-operation between the Federal Republic and the *Länder* in the areas of criminal investigation, for the establishment of a Federal Office of Criminal Investigation and for the international fight against crime. This does not mean the fight against international criminal offences but the fight against crime on an international level, like *e.g.* the co-operation of German and foreign authorities in criminal investigations. Apart from that, police law falls under the authority of the *Länder*, as it is concerned with the resistance to threats. Therefore, the question whether a required separation between the police and the intelligence services can be derived from the legislative competencies is not of importance in this context (also cf. BVerfGE 97, p. 198 [at p. 217]). 199

From all this, it follows that the challenged regulations must be embedded in a context of regulation and use that refers to foreign surveillance for them to arise out of the legislative competence from Article 73 no. 1 of the Basic Law. Contrary to this, Article 73 no. 1 of the Basic Law does not entitle the Federal parliament to confer authority to the Federal Intelligence Service that is aimed at preventing, hindering or prosecuting criminal offences as such. This does not preclude the possibility that parallel or overlapping activities may exist in the various areas of observation and information, as long as the missions and activities of the different agencies, which are clearly delimited by the division of authority, remain separate. 200

b) The regulation in § 1.1 and § 3.1 sent. 2 nos. 1 to 6 of the 1994 Fight against Crime Act can be identified as belonging to the legislative competence over foreign affairs. This is obvious as regards the threat of an armed aggression (no. 1), which, apart from this, also belongs to the area of competence over defence, but also applies to the areas of threat specified under nos. 2 to 6. 201

Certainly, the doubts that the complainants have expressed concerning the authority of the Federal parliament do not lack all merit. The new areas of threat have, in fact, been integrated into the G 10 Act in the framework of the Fight against Crime Act. Moreover, they are defined by specified activities that are relevant under criminal law, albeit not by elements of criminal offence as in § 3.3 of the G 10 Act. Moreover, § 3.5 of the G 10 Act obliges the Federal Intelligence Service to transfer information that is relevant under criminal law to authorities concerned with crime prevention and prosecution. Finally, the preparatory materials to the law in question contain statements that provide indications that the Federal Intelligence Service was expected to be involved in the fight against crime. 202

In spite of this, the surveillance of foreign threats is the most important aspect of the challenged regulation. Its primary objective is to gain intelligence for the mission of the Federal intelligence service. This becomes evident from the wording of the Act. § 1.1 no. 2 of the G 10 Act explicitly inserts telecommunication surveillance conducted for the objectives of § 3.1 sent. 2 nos. 2-6 of the G 10 Act in the framework of the mission of the Federal Intelligence Service pursuant to § 1.2 of the Federal Intelligence Service Act (BNDG). The mission consists in collecting and evaluating the information required for the gathering of intelligence about foreign countries that is of importance for the foreign and security policy of the Federal Republic of Germany. This conferral to the Federal Intelligence Service of the authority to conduct such monitoring is followed by an autonomous context of regulation and use that is based upon § 3.4 of the G 10 Act and §§ 2, 4, 12 of the BNDG, but is independent of the fight against crime. This context of regulation and use is determined by the mission of the Federal Intelligence Service. According to this regulation, the intelligence gathered is to be converted into situation reports, analyses and reports on individual events that are addressed to the Federal government. It is intended that they will enable the Federal government to timely recognise situations of threat and to counteract them politically. 203

The individual threats identified in § 3.1 sent. 2 nos. 2-6 of the G 10 Act also show the required relation to the foreign and security policy interests that the Federal Republic of Germany must safeguard as a member of the community of states and in its relation to intergovernmental institutions. Acts of weapons proliferation, arms trade, international terrorism, drug export and money laundering occurring in this context, all of which are relevant under criminal law, cannot only be regarded as international crime. Rather, such activities are characterised by the fact that they often emanate from foreign states or foreign organisations whose operations are supported or tolerated by the state, and that such operations take on dimensions that require international counter-measures. The Federal Republic of Germany must, therefore, be in a position to shape its foreign and security policy and its international co-operation to combat these activities and, to be able to do so, requires the corresponding intelligence. This is also true with respect to its ability to act (*inter alia*, as a member of NATO). 204

Nor can it be said from the outset that the threat of counterfeiting committed abroad (no. 5) bears no relation to the foreign affairs to which Article 73 no. 1 of the Basic Law refers. Certainly, the relation to foreign countries is not an inherent feature of counterfeiting. Such relation, however, is established if counterfeiting occurs with the participation of foreign countries or if, due to foreign activities, it reaches a scale that threatens monetary stability in Germany. In these cases, counterfeiting cannot sufficiently be combated by criminal prosecution on the domestic territory but requires foreign policy reactions. 205

Finally, if the subject of the regulation falls under the category of foreign affairs, (this is determined by the primary objective of the regulation), the duty of the Federal Intel- 206

ligence Service to make, with certain prerequisites, the intelligence gathered in the framework of its mission available to other agencies for the fulfilment of their tasks remains, in principle, unchanged. To respect the boundaries of competence, the parliament must assure, to the extent that it bases its regulations on Article 73 no. 1 of the Basic Law, that the authorisations and the measures that are based on the various competencies still relate to the Federal Intelligence Service, and it must avoid the situation in which the primary function is eclipsed by other possible uses. This is done by: (1) determining the intended use in a sufficiently precise manner; (2) adequately binding the restriction of telecommunications privacy to a specified objective; (3) defining authority in such a way that it is in line with the objective; and (4) providing measures of protection that are adequate in the context of a specified objective.

2. The regulations in § 1.1 and § 3.1 of the G 10 Act also fulfil the prerequisites laid down by Article 10 of the Basic Law concerning the specificity and clarity of powers of encroachments upon telecommunications traffic. 207

In particular the parliament has determined, in a sufficiently specific and clear manner, the objectives for which telecommunications links may be monitored and for which the intelligence thus gathered may be used. The threatening situations that are supposed to be timely recognised by observation or monitoring are described precisely enough and are further specified by reference to other laws. The scope of monitoring is determined by its limitation to international wireless traffic. In view of the mission and the workings of intelligence services, it was not possible to further specify the prerequisites that must exist for monitoring to take place. 208

3. As regards substance, however, § 3.1 sent. 2 no. 5 of the G 10 Act disproportionately restricts telecommunications privacy. Apart from this, § 3.1(2) of the G 10 Act complies with the requirements of the principle of proportionality. 209

a) The objective of timely recognising and counteracting the threats specified under numbers 1 to 6 of the provision is a legitimate interest of the common good. It is true that the threats specified under nos. 2 to 6, which were newly incorporated into the law, do not carry the same weight as the threat of an armed aggression, which has from the outset been regarded as a legitimate reason for telecommunications monitoring (cf. BVerfGE 67, p. 157 [at p. 178]). Whereas such an aggression jeopardises the existence of the state, the well-being of the population and the freely chosen liberal order of the state, the newly incorporated threats, as a general rule, do not affect the existence of the state or its order in the same fundamental manner. They do, however, concern high-ranking public interests whose violation would result in serious damage to external and internal peace and to the legal interests of individuals, albeit to different degrees. 210

b) Telecommunications monitoring on the basis of § 3.1 of the G 10 Act is suitable for achieving the objective of the law. 211

The wide range of screening, which only in comparatively few cases is likely to yield 212

information, is no argument against suitability. On the legal level, it is sufficient if there is an abstract possibility that the permitted measures achieve the intended objective, *i.e.* if the measures are not unsuitable from the outset but may contribute to the desired success (cf. BVerfGE 90, p. 145 [at p. 172]). This is the case here.

The requirement of suitability is also sufficiently taken into account on the level of implementation. On the one hand, monitoring takes place in a series of procedural steps that, by rendering the measures more specific, may promote their suitability. The determination of specific telecommunications links and the ordering of restrictions on the privacy of telecommunications links are meant to establish a framework that delimits the monitoring measures. The monitoring measures take place in regulated procedures, the elements of which comprise, in particular: (1) the application by the Federal Intelligence Service (§§ 4.2 no. 2 and 4.3 of the G 10 Act), which requires a statement of reasons; (2) the determination of the search concepts, which according to the text of the law must be suitable for achieving the aims of telecommunications monitoring (§ 3.2[1] of the G 10 Act); and (3) (previous) supervision by the panel of parliamentarians and the G 10 Commission (§ 3.1[1], § 9.2 of the G 10 Act). On the other hand, monitoring is subject to subsequent control by the G 10 Commission, which is established pursuant to § 9 of the G 10 Act. The panel of parliamentarians established pursuant to § 9.1 of the G 10 Act is to be informed by the Federal Minister of the Interior, at intervals not greater than six months, about the state of implementation of the law. 213

The suitability of monitoring measures is not called into question by the fact that it is possible to encrypt messages. Certainly, as the independent, court-appointed expert Professor Dr. Pfitzmann pointed out in the oral argument, it is possible to acquire, at low prices, encryption technologies that effectively shield the content of communication against any third party taking note of it; if steganographic methods are used, it is not even possible to recognise that the communication is encrypted. For the use of encryption technologies, however, it is necessary that both sender and receiver have the key at their disposal. As a general rule, this is only the case if sender and receiver have a permanent relation. Normally, the use of these technologies is not considered if business relations are initiated or if the contact is only sporadic. 214

In some of the listed areas of threat, however, it is likely that exactly the individuals or organisations that are the targets of monitoring are, due to their high degree of organisation and their use of modern infrastructure, in a position to evade telecommunications monitoring whereas unsuspected individuals who cannot make use of encryption technologies (as is the case with journalists, in view of their working conditions) become subjects of monitoring. The Federal Intelligence Service itself has stated that the poor results of monitoring in the areas of international terrorism and drug trade can, *inter alia*, be explained by the use of code words. In the oral argument the Federal government countered the objection that monitoring is unsuitable by stating that practical experience had shown that only relatively few of the screened telecommunications links were encrypted. 215

This leads to the conclusion that the question whether monitoring for the objective of early recognition of the respective threats fails due to the use of encryption technologies cannot, at least according to the present state of knowledge, be answered on an abstract level but only on account of practical experience. On the legal level, the permitted measures are not unsuitable from the outset. On the level of implementation, the Federal Intelligence Service and the supervisory bodies that are involved pursuant to the procedural arrangements are to ensure that in spite of the possibility of encryption, the suitability of the measures in the areas of threat that are the subject of an order restricting telecommunications privacy is maintained. 216

c) The law is necessary for achieving its aims. There are no means available that are equally effective, which less significantly impair the holders of fundamental rights. In particular, the possibility of co-operation with the states in which the sources of the threats arise is not equally promising. This is, on the one hand, due to the fact that co-operation requires previous knowledge about relevant facts. On the other hand, this is due to the fact that in many cases the threats are caused or condoned by government authorities abroad. 217

d) The restrictions on the right to privacy in telecommunication traffic instituted pursuant to § 1.1 and § 3.1 of the G 10 Act (screening, recording, storage, comparison) are, in essence, proportional in the narrower sense. Only restrictions instituted for the objective of recognising counterfeiting committed abroad (no. 5) fail to meet this requirement. 218

aa) The principle of proportionality requires that a loss of the freedom that is protected by the Basic Law is not disproportionate to the objectives of public interest that are served by the restriction of the fundamental right in question. Due to the fact that the individual is integrated in the community and depends on the community, the individual must tolerate restrictions of his or her fundamental rights if they are justified by prevailing public interests (cf. *e.g.* BVerfGE 65, p. 1 [at p. 44] with further references). The parliament must, however, achieve an adequate balance between public interests and the interests of the individual. In this context, the important questions with respect to the fundamental rights of the individual are: (1) under what circumstances are which and how many holders of fundamental rights subject to impairments; and (2) what is the degree of intensity of these impairments? The standards for determining this include: (1) which thresholds for intervention have been created; (2) the number of persons affected; and (3) the intensity of the impairments. The intensity of the impairment, in turn, depends on: (1) whether the communication partners' identities remain anonymous; (2) which calls and (3) which contents can be screened (cf. *e.g.*, on the basis of the standard of Article 2.1 of the Basic Law in conjunction with Article 1.1 of the Basic Law, BVerfGE 34, p. 238 [at p. 247]); and (4) what disadvantages threaten, or are justly feared by, the holders of fundamental rights on account of the monitoring measures. On the other hand lie the considerations of the public interests, as determined by the weight of the aims and interests served by the telecommunications monitoring. The decisive factors in this context are, *inter alia*: (1) how great are 219

the dangers that are to be recognised with the help of telecommunications monitoring; and (2) how probable is their occurrence.

bb) Telecommunications privacy is seriously impaired by the challenged regulations. 220

It is not the case, however, as argued in the first constitutional complaint, that with the challenged regulations the parliament has completely eliminated the telecommunications privacy secured by Article 10 of the Basic Law. The challenged regulations, thus, have not affected the essence of the fundamental right and are therefore in compliance with Article 19.2 of the Basic Law. "Global and generalised monitoring" with respect to foreign surveillance, which is prohibited by the Basic Law, is also not permitted by the challenged regulations (cf. BVerfGE 67, p. 157 [at p. 174]). The challenged regulations also do not permit a screening of all the telecommunications contacts of specific holders of fundamental rights that is not bound to certain prerequisites. Rather, monitoring and recording pursuant to the challenged regulations is limited legally as well as factually. 221

The limitation is, first of all, apparent from the fact that, pursuant to sentence 1 of § 3.1(1) of the G 10 Act, only wireless international telecommunications traffic is subject to monitoring. Monitoring measures do not extend to domestic telecommunications traffic. Restrictions of telecommunications privacy may include line-bound traffic only in order to recognise the threat of an armed aggression, but not concerning the other threats which have been newly incorporated into the law (§ 3.1[3] of the G 10 Act). Wireless traffic, *i.e.* traffic that is transmitted via microwave or satellite, presently amounts to approximately ten per cent of the entire telecommunications traffic but will, according to the independent, court-appointed expert Professor Dr. Wiesbeck, continually increase due to technological progress. 222

Whether a specific act of communication takes place via line-bound or wireless telecommunications systems, is, according to the experts' statements, determined automatically depending on the capacity and capacity utilisation of the transmission routes and is therefore unpredictable for the communication partners as well as for the Federal Intelligence Service. For these reasons alone, comprehensive screening is not feasible, at least as far as the international telecommunications traffic is concerned. It is true that in any telecommunications contact abroad, the individual engaged in this contact must be aware of the possibility that the contact is screened by the Federal Intelligence Service. Such a screening will in actuality, however, only rarely occur. 223

As far as international wireless telecommunications contacts are concerned, the probability of screening is further diminished by the circumstance that, according to the information given by the expert Professor Dr. Wiesbeck, the uplink can, for technical reasons, only be observed to a limited extent so that, essentially, only the downlink is covered by monitoring efforts. According to the expert, it is technically possible to combine both communication elements, but this would require a large-scale co- 224

operation between the receiving installations in the uplink and in the downlink areas. These circumstances lead to the result that in the case of satellites with a bundled coverage area, only limited parts of an individual act of telecommunication can be screened and that contributions by both communication partners are only recorded by older satellites with a wide coverage zone.

Other limitations on the monitoring permitted by the challenged regulations result from the fact that, in order to initiate telecommunications monitoring it is necessary to determine the specific links and establish the monitoring thereof by specific orders. Furthermore, restrictions on telecommunications privacy resulting from monitoring will only occur if the threatening situation is sufficiently established by the Federal Intelligence Service and, in view of the Federal Intelligence Service's limited capacities, sufficient results are expected. It has become apparent in practice that considerations like limited resources and utility actually achieve a limiting effect: the orders concerning the areas of threat of international terrorism and drug trade, have, pursuant to § 5.3(2) of the G 10 Act not been renewed due to the poor results of the monitoring. 225

On the other hand, the assumptions that formed the basis of the Federal Constitutional Court's 1984 decision, which found the weight of the impairment of fundamental rights arising out of telecommunications monitoring to be relatively low (BVerfGE 67, P. 157), are no longer valid. In that decision the Federal Constitutional Court proceeded on the assumption that the determination of telecommunications links and the ordering of restrictions on the privacy of telecommunications traffic issued after consultation with the parliamentary panel, as required by law, would result in a strong geographic restriction of the monitored areas and to a strong restriction of the monitored routes (cf. BVerfG, *loc. cit.,* p. 174). Strategic surveillance was regarded as proportional, as the Court claimed that: (1) it serves an especially important objective, *i.e.* the prevention of an armed aggression against the Federal Republic of Germany; (2) there is very little probability that an individual will become the subject of surveillance; and (3) that surveillance places only a minor burden on the individual due to the fact that anonymity of the communication partners is, in principle, assured (cf. BVerfG, *loc. cit.,* pp. 178-179). 226

Certainly, telecommunications monitoring pursuant to § 3.1 and § 5.1 of the G 10 Act is still to be determined and ordered by the responsible Federal minister and requires approval by the parliamentary panel established pursuant to § 9 of the G 10 Act. The change of the factual and legal framework conditions has, however, considerably diminished the limiting effect these procedures can be expected to have on the encroachments on telecommunications privacy that are permitted by the challenged regulations. As long as strategic surveillance of telecommunications, as based on the original version of the G 10 Act, only referred to the threat of an armed aggression against the Federal Republic of Germany and as long as, according to political analysis, such an aggression only emanated from the Eastern Block, surveillance was restricted to the countries of the Warsaw Pact. Moreover, an order for monitoring under the previous regime, under the existing technical conditions, always referred to indi- 227

vidual routes of communication, so-called corridors, *e.g.* specific collective cables for the transfer of long-distance calls to the respective area.

Meanwhile, the incorporation of nos. 2 to 6 into the G 10 Act has considerably increased the quantity of threats about which intelligence should be gathered. Consequently, surveillance is no longer restricted to a single crisis region. This means that the geographical area that may be covered by monitoring measures has been considerably expanded. The observation of satellite radiuses has considerably increased the volume of screened telecommunication traffic links. Under these circumstances, mainly the search concepts as defined by § 3.2 of the G 10 Act that are approved in the order establishing the monitoring measures, which control the selection of the monitored telecommunications contacts, serve to limit surveillance. 228

Finally, the anonymity of the act of communication is no longer assured as was the case under the previous regime. It is true that the search concepts as defined by § 3.2 of the G 10 Act, apart from the exception in sent. 3 that is not under review here, may not contain any characteristics for identification that result in the targeted screening of specific acts of telecommunication traffic. This prohibition, however, no longer shields the subscriber lines to which it applies from the identification of the subscribers in the same way as it used to do. One reason for this is that, due to the development of technology, the information regarding the circumstances of an act of communication, including the parties' identities, is also gathered and retained. On the other hand, the identification of individuals now results from the fact that the threats that have been newly incorporated into the Act are, to a far greater extent, related to specific individuals than was the case with respect to the threat of war. Furthermore, the Federal Intelligence Service concedes that monitoring often only yields the desired intelligence if the identity of the individual communication partners is disclosed. 229

In present practice, the Federal Intelligence Service, according to its own statements in the oral argument, mainly monitors the telex and fax traffic that is routed via telecommunications satellites. The Federal Intelligence Service claims that telephone traffic is only monitored to a very limited extent, communication via radio is, as of yet, not being monitored at all. According to the considerations presented in the oral argument, the Federal Intelligence Service plans to expand monitoring to e-mail traffic. Pursuant to the information provided by the Federal Intelligence Service, the essence of which was not challenged in a substantial way at the oral argument, approximately 15,000 acts of telecommunications traffic are processed by the conversion devices every day. Pursuant to the legal opinion that Article 10 of the Basic Law and the G 10 Act are not relevant in this context, 14,000 of them are classified as falling under the tasks regulated in § 1 of the *Gesetz über den Bundesnachrichtendienst* (BNDG, Federal Intelligence Service Act). Apart from that, approximately 700 acts of telecommunications traffic fall under the G 10 Act, 70 contain search concepts and are processed by Federal Intelligence Service staff, 20 appear to be relevant and are evaluated. The present extent of screening is, however, not prescribed by the Act but above all determined by the existing technical and personal capacities and can there- 230

fore be expanded without a violation of the law.

When judging the intensity of the impairment of fundamental rights, it is important that every participant in international telecommunications traffic is exposed to the monitoring measures whether or not there is a relationship between the monitoring and his or her behaviour and whether or not the monitoring was provoked by his or her behaviour. As regards content, acts of communication of all kinds are screened in their entirety. In this context, it is possible that Federal Intelligence Service staff takes note of the communication. In this respect, the fact that the search concepts, due to the state of technological development, only insufficiently fulfil the function that is assigned to them by the parliament, *i.e.* to make human access to the obtained material unnecessary until comparison has taken place, shows its effects. 231

According to the statements of the Federal Intelligence Service, which have been confirmed by the experts, only in the exceptional case of telex monitoring is fully automatic comparison of search terms feasible. Telex traffic, however, is less and less frequent. Contrary to this, fax traffic can only be automatically compared and reviewed to a limited extent and telephone traffic cannot be automatically compared and reviewed at all. This explains why most intelligence, by far, is gathered by means of so-called formal search concepts (foreign subscriber numbers) based on the exemption provision of § 3.2(3) of the G 10 Act. According to the statement of the expert Professor Waibel, voice recognition procedures cannot yet be effectively employed, in spite of their continuous improvement, in the implementation of the G 10 Act nor will they be effective in the near future without human contribution. Independent of the practice of the Federal Intelligence Service, the Act does not preclude that the comparison is done by staff, even though the parliament may have imagined comparison taking place automatically. 232

When judging the intensity of the impairment of fundamental rights, the lack of anonymity of the participants in a communication is to be considered as well. The fact that the intelligence gathered relates to specific individuals is not restricted to the screening and recording phase. In practical work with the intelligence gathered, this relation is preserved. According to the statements of the Federal Intelligence Service, this is necessary, in some of the cases, in the framework of evaluation, to assess and classify the intelligence. The Federal Intelligence Service eschews the use of technically possible temporary memory systems that would allow it to access the information regarding the circumstances of the call, including the parties' identities, only if it proves necessary to make use of information regarding the individuals involved in the communication contact in order to fulfil the tasks of the Federal Intelligence Service. 233

The risks that can objectively be expected or must be feared begin to emerge as early in the monitoring process as that point when the Federal Intelligence Service takes note of an act of communication. In fact, even before the Federal Intelligence Service takes note of acts of communication, the fear of being monitored, (and of the dangers of recording, subsequent evaluation, possible transfer and further utilisation 234

by other authorities, that are connected with monitoring), may lead to inhibitions in communication, to communication disturbances and to the individual adapting his or her behaviour, in this context especially in order to avoid specific contents of conversation or specific terms. In this context, not only the individual impairment of a large number of holders of fundamental rights must be taken into consideration. Rather, the secret monitoring of telecommunications traffic concerns the communication of society as a whole. Therefore, the Federal Constitutional Court has stated that the right to informational self-determination, which is comparable in this respect, also bears a relation to the common good that goes beyond the interest of the individual (cf. BVerfGE 65, p. 1 [at p. 43]).

cc) On the other hand, it is of importance that the restrictions of fundamental rights serve to protect high-ranking public interests. 235

Monitoring measures based on § 3.1(1) and § 3.1 sent. 2 no. 1 of the G 10 Act are supposed to yield intelligence about facts that are relevant under defence policy aspects so that threats to the Federal Republic of Germany involving armed aggression can be timely recognised. It is true that the nature of such a threat has changed with the dissolution of the Warsaw Pact. The Act, however, is not bound to the historical constellation that the parliament had in mind when enacting the law. Rather, the telecommunications monitoring regime can still be applied even if the threat that such measures are intended to counteract has shifted. This is true in the case of the threat of armed aggression. Even after the dissolution of the Warsaw Pact, this threat still exists. 236

In the new areas of monitoring, increased threats have developed due to the increase of internationally organised crime, in particular in the area of illegal trade with weapons of war and with drugs as well as in the area of money laundering. Even if such activities cannot, altogether, be put in the same category of importance as armed aggression aimed at the Federal Republic of Germany, they considerably affect, in any case, the foreign and security policy interests of the Federal Republic of Germany. Nor are the threats in the specified areas remote. In the area of weapons proliferation, the Federal government has furnished sufficient examples that are generally known. 237

The threats, the sources of which are predominantly located abroad and which are supposed to be detected by means of the authority to restrict telecommunications privacy, are of great importance. This still applies to the threat of armed aggression but also, as has been sufficiently established by the Federal Intelligence Service, to the threats of weapons proliferation, arms trade, and international terrorism. The aim behind the mission of foreign surveillance, *i.e.* to provide the Federal government with information that is of foreign and security policy interest for the Federal Republic of Germany, is of considerable importance if the Federal Republic of Germany is to act effectively in the field of foreign policy and maintain the reputation of its foreign policy. 238

dd) In a weighing of interests that takes these aspects into consideration, § 3.1 sent. 2 nos. 1-4 and no. 6 of the G 10 Act are not objectionable from the constitutional point of view. 239

Contrary to the opinion of the complainant bringing the first constitutional complaint, the authority to monitor and record, and the other measures provided by the challenged Act is not out of proportion simply because it lacks intervention thresholds like the traditional concepts of *konkrete Gefahr* (specific threat) in the field of resistance to threats and of *hinreichender Tatverdacht* (reasonable grounds for the suspicion of a criminal act) in the field of criminal prosecution. Certainly, telecommunications monitoring is conducted without an existing suspicion. Neither is the encroachment upon fundamental rights limited to the general risk that the individual may become the subject of an unjustified suspicion. In the framework of determining and ordering restrictions to telecommunications privacy, anyone can easily become the object of monitoring measures. 240

The different aims, however, justify that the prerequisites for encroachments on telecommunications privacy are determined differently in the G 10 Act than in police law and law of criminal procedure. On account of the legislative power of the Federal Republic of Germany flowing from Article 73 no. 1 of the Basic Law, the only possible aim of monitoring by the Federal Intelligence Service is foreign surveillance with respect to specified threatening situations that are relevant to foreign and security policy. This type of surveillance shows the following characteristics: (1) it is concerned with the external security of the Federal Republic of Germany; (2) its subject is threatening situations that originate abroad, not predominantly threatening situations and suspected threats that are related to individuals; and (3) intelligence in this respect can only to a limited extent be obtained by other means. In this context, the Federal Intelligence Service's sole mission is to collect and evaluate the information required for obtaining intelligence about foreign countries that are of importance for the foreign and security policy of the Federal Republic of Germany, and, on account of its duty to inform the Federal government, to provide it with information to support it in its decisions. 241

It is true that even the considerable threats, which telecommunications monitoring is supposed to counteract, would not justify, from the constitutional point of view, telecommunications monitoring for objectives of foreign surveillance without any prerequisites or limitations. The law, however, has not dispensed with such prerequisites. §§3.1(1) and 3.1(2) of the G 10 Act contain specified substantive standards and procedural safeguards, chiefly that monitoring is only permissible for collecting information about issues the knowledge of which is necessary for the timely recognition of the threatening situations. Under the procedural aspect, one of the prerequisites of the determination and ordering of monitoring is that the Federal Intelligence Service, in its application, conclusively establishes why the affected telecommunications links can provide, in a timely manner, information about one of the relevant threats. 242

Taking into account the safeguards provided in the G 10 Act, screening and recording for the objective of informing the Federal government do not appear to be disproportionate. Certainly, the number of screened telecommunications links is not low, it is low, however, compared with the total number of telecommunications contacts, or even in comparison only with the number of international telecommunications contacts. In this context, the ban on targeted monitoring of specified individual subscriber lines contained in § 3.2(2) of the G 10 Act is of great importance. In view of the fact that encroachments on telecommunications privacy are implemented without the existence of a suspicion, in view of the broad range of screened telecommunications contacts and of the possibility of identifying the participants in a telecommunications contact, proportionality would not be ensured without such a ban. The Federal Constitutional Court is not called upon to review the constitutionality of § 3.2(3) of the G 10 Act because the complainants who have lodged admissible constitutional complaints are not affected by this regulation. Even if free communication, which Article 10 of the Basic Law is supposed to ensure, may be disturbed by the screening and recording of acts of telecommunication, the danger of disturbing it gains its full significance only through subsequent evaluation and especially by the transfer of the gathered information. In this respect, however, it can be adequately counteracted on the level of the authority to evaluate and transfer. 243

ee) Proportionality in the narrower sense is not ensured, however, with respect to the threat of counterfeiting committed abroad, which is listed under no. 5 of the regulation. 244

Counterfeiting is neither a threat the seriousness of which is comparable to the threat of armed aggression, nor does it concern legal interests that are as important as the other threats incorporated into § 3 of the G 10 Act by the 1994 Fight against Crime Act. Counterfeiting also does not show, in all its forms of perpetration, the same potential for danger that characterises the other threats. Counterfeiting neither constitutes a threat to the existence or the safety of the Federal Republic of Germany that is necessarily connected with foreign countries nor is it necessarily a considerable threat to the existence or the safety of the Federal Republic of Germany. This does not preclude that in individual cases, large-scale counterfeiting committed abroad impairs the Federal Republic of Germany's monetary stability, and thus its economic performance, to a degree that is comparable to the other threats. The provision, however, is not limited to such cases. With respect to the threat posed by counterfeiting generally, the degree of the threat and the weight of the impairment of fundamental rights is out of proportion. 245

By incorporating respective limitations, however, § 3.1 sent. 2 no. 5 of the G 10 Act can be given a wording that is consistent with the Basic Law. This part of the regulation is therefore not to be declared void but is only to be declared inconsistent with the Basic Law. The parliament is obliged to create consistency with the Basic Law. 246

IV.

The provision of § 3.4 of the G 10 Act, which obliges the Federal Intelligence Service to examine whether the personal data obtained by telecommunications monitoring is required for the objectives that justify these measures is not objectionable from a constitutional point of view when considered by itself. This provision does not sufficiently take account of the requirements, which follow from Article 10 of the Basic Law, that: (1) an infringement upon telecommunications privacy be bound to a specific use; and (2) that an infringement upon telecommunications privacy be proportional. To this extent, this provision is inconsistent with telecommunications privacy and the freedom of the press (which is to be considered alongside telecommunications privacy). 247

It is true that § 3.4 of the G 10 Act complies with the principle that an infringement upon the right to telecommunications privacy be bound to a specified purpose to the extent that this provision of the G 10 Act requires that the Federal Intelligence Service examine whether the data that is obtained by means of telecommunications monitoring is suitable for a specified objective. Apart from that, this principle is observed by the fact that § 3.6(1) of the G 10 Act orders the destruction or deletion of the data if the examination has shown that the data is unnecessary for the objectives of the Federal Intelligence Service. The Act, however, does not sufficiently ensure that the use of the data that is not destroyed or deleted is bound to the objective that justified the collection of data in the first place. Possible uses other than the early recognition of the threats specified in the Act and the corresponding provision of information to the Federal government are not excluded. The regulations provided by the Federal Intelligence Service Act, which address the processing and utilisation of personal data, cannot fill this gap. § 11 of the Federal Intelligence Service Act excludes the application of the general provisions in § 14 of the Federal Data Protection Act for which the storage, modification and use of obtained data is permissible. Apart from this, § 3.4 of the G 10 Act does not acknowledge the duty, which follows from Article 10 of the Basic Law, to identify and mark the object of protection of fundamental rights to make it possible to track the object of fundamental rights protection throughout the remaining steps of processing. 248

Nor does the challenged regulation make the further evaluation of the data dependent on meeting a threshold of proportionality. § 3.3 of the G 10 Act, which establishes specified requirements for the utilisation of the data, makes no reference to the Federal Intelligence Service. Instead, the provision’s objective (the prevention, resolution or prosecution of criminal offences identified by this article) is addressed to the authorities to which the Federal Intelligence Service, pursuant to § 3.5 of the G 10 Act, is to transfer information. The Act does not contain provisions that ensure that the Federal Intelligence Service evaluates only the data obtained by telecommunications monitoring that shows a sufficient relevance to the work of the intelligence service for the areas of threat specified in §§ 1.1 and 3.1 of the G 10 Act. The fact that such a threshold is lacking is also of importance with regard to Article 5.1(2) of the Ba- 249

sic Law because such a threshold would ensure that the Federal Intelligence Service takes the interests of the protection of informants and of the confidentiality of editorial work into account.

An interpretation of the provision that is consistent with the Constitution is not possible as it would not be in conformity with the requirements of specificity and clarity placed on legal regulations by Article 10 of the Basic Law. The challenged provision only requires amendment; its deficiencies do not result in the provision being void but only result in its inconsistency with the Basic Law. The parliament is obliged to create consistency with the Basic Law. 250

V.

§ 12 of the Federal Intelligence Service Act obligates the Federal Intelligence Service to report to the Federal government the content of the data obtained pursuant to its telecommunications monitoring activities. This obligation is challenged in these proceedings only to the extent that § 3.3(2) of the G 10 Act excludes the reporting obligation from the requirements of § 3.3(1) of the G 10 Act. In the framework of the Federal Intelligence Service's obligation to report to the Federal government, telecommunications privacy is not sufficiently protected. 251

The effect of Article 10 of the Basic Law and Article 5.1 of the Basic Law (to the extent that acts of communication fall under the freedom of the press) also extends to the Federal Intelligence Service's duty to inform the Federal government of its telecommunications monitoring activities because informing the Federal government is one of the objectives for which the Federal Intelligence Service has been granted the right to conduct telecommunications monitoring. The protection provided by the obligation to report to the Federal government by no means becomes unnecessary simply because personal data obtained as a result of monitoring is judged to be of no importance as regards the fulfilment of the duty to inform the Federal government. The duty to inform the Federal government not only requires that the Federal Intelligence Service draw up situation reports. The Federal Intelligence Service is, as § 12 of the Federal Intelligence Service Act explicitly emphasises, authorised to transfer personal data. 252

It certainly cannot be criticised that § 3.3(2) of the G 10 Act excludes the duty to inform the Federal government established by § 12 of the Federal Intelligence Service Act from the limitations of use pursuant to § 3.3(1) of the G 10 Act, as the limitations provided in this sentence are not geared to the tasks of the Federal Intelligence Service. It is, however, inconsistent with Article 10 of the Basic Law that this provision also does not provide that telecommunications monitoring be bound to the objectives established in § 1.1 and in §§ 3.1(1) and § 3.1(2) of the G 10 Act that justify telecommunications monitoring. Moreover, the absence of an obligation to mark personal data constitutes a violation of Article 10 of the Basic Law. 253

Nor are there any corresponding safeguards as regards the Federal government. 254

The protection Article 10 of the Basic Law provides is not limited to acts of the Federal Intelligence Service as the body that collects the data but also extends to acts of the Federal government as the body that receives the data. The holders of fundamental rights have an even greater need for protection *vis-à-vis* the Federal government than *vis-à-vis* the Federal Intelligence Service. Whereas the mission of the Federal Intelligence Service is limited to observing and evaluating events without having executive powers, the Federal government, as a political body and as the executive head of the state on the national level, has means to make use of its knowledge through measures that can considerably impair persons who are affected by telecommunications monitoring.

The Federal government, which is to be informed by the data obtained through monitoring, may therefore not use the data at its discretion. It is only permissible for the Federal government to take note of the content or the circumstances of telecommunications contacts in order to be in a position to timely recognise the threats specified in § 3.1 sent. 2 nos. 1-6 of the G 10 Act and to take measures to counteract them. The Federal government is therefore not allowed to store or use the data for other objectives. 255

As the challenged provision, considered on its own, does not contradict the constitution but only requires amendment, its deficiencies also do not result in the provision being void but only results in its inconsistency with the Basic Law. The parliament is obliged to create consistency with the Basic Law. The Basic Law leaves the decision about the precise place in which this duty is fulfilled to the legislative discretion of the Federal government. 256

VI.

The provision of § 3.5(1), in conjunction with § 3.3(1) of the G 10 Act, that obliges the Federal Intelligence Service to transfer data obtained by telecommunications monitoring to other authorities for the execution of their duties is not entirely consistent with the provisions of Article 10 of the Basic Law and the complementary provisions of Article 5.1(2) of the Basic Law. 257

1. The objective of the regulation, however, is not objectionable from the constitutional point of view. The data and information that the Federal Intelligence Service has obtained from telecommunications traffic when fulfilling its mission, are supposed to be utilised for the prevention, resolution or prosecution of criminal offences to the extent that they indicate offences committed by specified individuals. The Basic Law confers great importance to the prevention and resolution of criminal offences. The Federal Constitutional Court has therefore repeatedly emphasised the irrefutable requirement that criminal offences be effectively prosecuted and of an effective fight against crime. The Federal Constitutional Court has also repeatedly stressed the public interest in the truth being ascertained as completely as possible in criminal proceedings, for the conviction of offenders as well as for the exoneration of the innocent, and has described the effective resolution especially of serious criminal of- 258

fences as an important mission of a polity governed by the rule of law (cf. BVerfGE 77, p. 65 [at p. 76] with further references; BVerfGE 80, p. 367 [at p. 375]).

2. The parliament has also complied with the requirement that it determine, precisely and specifically for each area, the objectives for which personal data may be transferred and further used (cf. BVerfGE 65, 1 [at p. 46]). This provision permits a transfer of data to the receiving agencies specified in § 3.5 of the G 10 Act only to the extent that this is required for the execution of the receiving agency's duties. Thus, the provision refers to the intelligence service tasks, the administrative and monitoring duties and the missions of crime prevention, of the resistance to threats and of the prosecution of criminal offences that are assigned to the respective receiving agencies. § 3.3(1) of the G 10 Act further delimits the objectives of use, in the framework of these agencies' tasks, to the prevention, resolution or prosecution of the listed criminal offences. 259

3. Moreover, the objectives justifying the transfer of data are consistent with the objective for which a restriction of telecommunications privacy has already taken place, and which resulted in the collection of data (cf. BVerfGE 65, p. 1 [at p. 62]). 260

It is true that the Federal Intelligence Service's telecommunications monitoring without an existing suspicion is only permissible for strategic surveillance. The characteristic feature of this type of monitoring is that its aim is not to initiate measures against specific individuals but that it concerns threatening situations on an international level about which the Federal government is supposed to be informed. Only this limited objective justifies such a broad scope and the depth of encroachment upon fundamental rights that results from monitoring without an existing suspicions. If the monitoring were, from the outset, justified by efforts aimed at the prevention or prosecution of criminal offences, the power to conduct such monitoring would not be consistent with Article 10 of the Basic Law (cf. BVerfGE 67, p. 157 [at pp. 180-181]. Limitations on employing specified methods of collecting data, which are required by fundamental rights, may not be evaded by making legally gathered data available for objectives that would otherwise not justify monitoring. 261

Article 10 of the Basic Law does not, however, exclude all transfers of data to agencies that may not or should not be permitted, on their own, to conduct telecommunications monitoring without an existing suspicion. As the Federal Intelligence Service, on account of the liberal methods it is permitted to employ, necessarily screens a large number of acts of telecommunication that are from the outset irrelevant for the receiving agencies, it must, in any case, be ensured that these agencies are not permitted to access the complete stock of data. On the other hand, it does not contradict the primary objective for which the data is collected if information that is relevant to the prevention, resolution or prosecution of criminal offences (although it has been collected with different objectives in mind) is transferred to the agencies mentioned under § 3.5 of the G 10 Act after careful examination of the data by the Federal Intelligence Service. The provisions of the challenged regulation that govern the transfer of data com- 262

ply with the requirements that must be met in this context: *i.e.* a threshold for the transfer that is established in § 3.5(1) as well as in § 3.1(1) of the G 10 Act, and a particular review by an official who is qualified to hold judicial office established in § 3.5(2) of the G 10 Act.

4. The challenged provisions are, on the other hand, not fully consistent with the principle of proportionality. 263

a) What is lacking, however, is not the suitability and necessity of the regulation for achieving the desired objective. 264

It is obvious that the transfer of data to agencies whose mission is, *inter alia*, the prevention, resolution or prosecution of criminal offences, aids the fulfilment of this mission. Nor has the circle of receivers been expanded to include agencies that cannot contribute to achieving the objective of the Act. Those agencies that are not entrusted with tasks concerning the prosecution of criminal offences but only perform administrative or intelligence services functions, have, in any case, within the boundaries of their mission, the possibility to prevent criminal offences. 265

There is no apparent means that would constitute a less intrusive encroachment while at the same time promising similar chances for success. Within the boundaries set by the authority they have been granted, the receiving agencies could not otherwise receive this information, which the Federal Intelligence Service can acquire due to its broader authorisation to monitor telecommunications. Moreover, the parliament has ensured compliance with the principle of necessity by limiting the duty to transfer data to that data which is necessary for the execution of the receiving agency's duties. 266

b) The parliament, however, has not complied with the requirements that the principle of proportionality, in its narrower sense, places on regulations that permit encroachment upon fundamental rights. 267

aa) The more narrowly construed principle of proportionality prohibits encroachments upon fundamental rights of an intensity that is out of proportion to the importance of the matter and the harm the individual citizen must suffer (cf. BVerfGE 65, p. 1 [at p. 54]). Rather, an adequate relationship between the importance of the fundamental rights in question and the seriousness of the restrictions on these fundamental rights must be established. In an overall balancing between the severity of the encroachment on the one hand, and the importance and urgency of the reasons that justify the encroachment on the other hand, the bounds of reasonableness must still be respected (cf. BVerfGE 67, p. 157 [at pp. 173, 178]; established case law). 268

The severity of the encroachment upon telecommunications privacy that results from the transfer permitted by the G 10 Act is best characterised by the fact that the transfer of personal data constitutes another break of telecommunications privacy that can result in an even greater impairment than the original encroachment (that took place with the monitoring). The effect of data transfer is not limited to the expan- 269

sion of the group of persons that obtain knowledge of the circumstances and the content of an act of telecommunication. Taking note of an act of telecommunication may precede measures taken against the subjects of monitoring. The Federal Intelligence Service cannot take any measures that are directed against individuals, and the Federal government, which the Federal Intelligence Service is to inform about specified threatening situations, does not take measures against the participants in an act of communication in the framework of its political counter-strategies. But the agencies to which the data is to be transmitted pursuant to § 3.5(1) of the G 10 Act will, as a general rule, institute investigations against the subjects of monitoring that may lead to further inquiries and, as the case may be, to the institution of criminal proceedings.

In this context it is also of importance, for judging the intensity of the encroachment, that the Federal Intelligence Service has obtained the information by means of a method that, due to the broad scope of its power to monitor telecommunications, including the power to conduct monitoring that is not motivated by suspicion, very severely affects telecommunications privacy. This is only consistent with Article 10 of the Basic Law because it merely serves strategic objectives and requires the identification of the participants in an act of communication only to facilitate the interpretation of the information, which is always fragmentary and therefore requires interpretation. Under these circumstances, the acceptability of the transfer of data to the designated agencies can only be ensured if the interests served by the transfer prevail over telecommunications privacy and if there is a safe basis for the assumptions that: (1) the data is relevant to these interests; and (2) that the persons affected by monitoring are, with sufficient probability, involved in criminal offences. If this basis is lacking, the bounds of what is reasonable have been transgressed. 270

It is therefore imperative that the legal interest (the prevention, resolution and prosecution of the listed criminal offences) justifying the transfer be of great importance. A sufficient factual basis for the suspicion that criminal offences are being planned or have been committed is also imperative. A lower degree of probability (with respect to a possible or actual violation of the applicable legal interest) justifies transfer when the legal interest at stake is very important. Similarly, less cogent facts may form the basis of a suspicion justifying transfer when the legal interest at stake is very important. 271

The more important the legal interest is, the further the threshold for transfer may be shifted to a point in time prior to the threatening violation of a legal interest. In order for acts of planning, together with the prerequisite of the existence of factual grounds, to be sufficient to serve as a threshold for the transfer of data, the legal interest must be of outstanding importance (cf. BVerfGE 30, p. 1 [at p. 18]). This means that if the parliament confines itself to a few high-ranking legal interests when identifying the applicable legal interests and ascertaining if the damage that threatens them is extraordinarily high, the parliament is not hindered from keeping the threshold for transfer relatively low. If the parliament, on the contrary, considerably expands the catalogue of protected legal interests and also includes acts that show a low degree of threat in 272

the success that is to be prevented, it must set a high threshold for transfer.

bb) The parliament has not, in all respects, achieved this state of balance with regard to the elements of a criminal offence that justify the transfer of data. Certainly § 3.5 in conjunction with § 3.3 of the G 10 Act is not objectionable to the extent that it permits data transfer regarding persons against whom restrictions of telecommunications privacy pursuant to § 2 of the G 10 Act have been ordered. To the contrary, the scope of the elements of a criminal offence is not sufficiently delimited with respect to suspicion-related restrictions. This results from the interplay between the catalogues of relevant criminal offences, the factual basis for the suspicion of criminal offences and the duration of the threat to the legal interest. 273

The catalogue of criminal offences for the prevention, resolution or prosecution of which the Federal Intelligence Service may transfer to other agencies personal data obtained from telecommunications monitoring is extraordinarily heterogeneous. It is not limited to major criminal offences but also includes minor criminal offences. On the one hand, it contains criminal offences that damage the highest-ranking public interests or even threaten the ability of the state to protect legal interests as a whole. In part, they correspond in their importance to the criminal offences that, pursuant to § 2 of the G 10 Act, justify the ordering of measures of telecommunications monitoring against specified persons or even exceed these criminal offences in importance. Included among such criminal offences are, for example, causing an explosion by nuclear energy (§ 310b of the StGB [*Strafgesetzbuch*, German Criminal Code]), to which reference is made in § 138 of the StGB. Other criminal offences, however, involve a less serious level of criminality, *e.g.* minor cases of counterfeiting eurocheque forms (§ 152a.2 of the StGB), to which reference is also made in § 138 of the StGB, or fraud regarding eligibility for a subsidy (§ 264 of the StGB), which is mentioned in § 3.3(1) of the G 10 Act. 274

Moreover, the factual basis that must exist in order to justify the suspicion of criminal activity and thereby permitting the transfer of data pursuant to the G 10 Act, is relatively low in comparison with the factual basis justifying the suspicion of criminal activity and thereby telecommunications monitoring pursuant to § 100a StPO (*Strafprozessordnung* [Code of Criminal Procedure]). § 100a of the StPO requires "*bestimmte Tatsachen* " (specific facts) to justify the suspicion that someone has committed or is committing criminal offences or, if the attempt is punishable, has attempted to commit or is attempting to commit such criminal offences or has prepared to commit such criminal offences by means of another criminal offence. *Tatsächliche Anhaltspunkte* (factual grounds), however, are sufficient to justify the transfer of data pursuant to § 3.5 in conjunction with § 3.3 of the G 10 Act. Finally, the inclusion of the planning phase that precedes the punishable attempt pursuant to § 100a of the StPO extends the possibility of data transfer to the lead-up of criminal offences, which involves a nearly unlimited range of activity. 275

This results in different consequences for the prevention of criminal offences on the 276

one hand and for the resolution and prosecution of criminal offences on the other hand. These consequences spring from the fact that data transfer for the protection of legal interests can show different degrees of urgency. Whereas the prevention of criminal offences is part of the resistance to threats and is meant to protect the affected legal interest from threatening violation, *i.e.* is supposed to prevent success, the prosecution of criminal offences is aimed at the state sanctioning the violation of a legal interest that has already taken place and can no longer be prevented. If a telecommunications contact that is screened by the Federal Intelligence Service contains indications concerning the planning as well as the completion of criminal offences contained in the catalogue of § 3.3(1) of the G 10 Act, this can, consequently, lead to a different legal assessment of a transfer carried out pursuant to § 3.5 of the G 10 Act.

277 Because, in the case of the prosecution of a criminal offence, the violation of the legal interest has already taken place and the focus is now on sanctioning it, it is not justified to lower the threshold for the transfer of personal data that was obtained by means of encroachments upon telecommunications privacy pursuant to §§ 1 and 3 of the G 10 Act below the threshold that otherwise applies to encroachments upon telecommunications privacy pursuant to § 100a of the StPO in crime prosecution. In the case of the transfer of the data collected by the Federal Intelligence Service, it appears necessary from the constitutional point of view, with regard to the fact that encroachment in this case is no less serious, to establish the requirement of a factual basis for the suspicion that corresponds to the one prescribed by § 100a of the StPO. Otherwise, the number of holders of fundamental rights affected could not be kept within the bounds of what is reasonable. § 3.3(1) of the G 10 Act does not comply with this requirement. It lowers the threshold for transfer below the bounds of what is reasonable by establishing that factual grounds for the suspicion that criminal offences have been committed are a sufficient standard for the transfer of data, a standard, however, which is considerably lower than that established by § 100a of the StPO.

278 To the extent that the prevention of criminal offences is concerned, the regulation does not comply with the interests that are protected by the Basic Law. All in all, the following circumstances result in a marked imbalance to the detriment of the fundamental rights affected: (1) that factual grounds are sufficient for a suspicion; (2) that the planning phase is included in the consideration; and (3) that less serious criminal offences also justify the transfer of data. In particular, a result of the circumstance that factual grounds are connected with the planning of criminal offences is that the power to monitor sets in at very early, preliminary stages of the threatened violation of a legal interest, which results in lowering the degree of probability and the certainty of predictions. Another consequence is that the power to monitor may be based on relatively low requirements as regards the factual basis.

279 Therefore, the parliament cannot make statutory provision for the consideration of all the competing elements of the regulation concerning the transfer of data for the

objectives of the prevention of crime. If the factual basis chosen by the parliament and the extension of the power to monitor to the planning phase of a criminal offence are considered together with the catalogue of criminal offences that justifies the use of the Federal Intelligence Service's information, the two prerequisites that are listed first can only be constitutional if the catalogue of criminal offences is further restricted. The broad scope of the catalogue of criminal offences can, however, only be justified if the prerequisites regarding the certainty of predictions are higher. Moreover, the element of a "*tatsächlicher Anhaltspunkt*" (factual ground) can, in its essence, only comply with the constitutional prerequisites if a restrictive interpretation ensures that a factual basis more than mere assumptions for the suspicion exists in the shape of circumstances that are concrete and, to a certain extent, condensed.

Nor are the precautions for the protection of telecommunications privacy completely sufficient from the constitutional point of view. Certainly, a regulation that goes beyond § 3.5(2) in that it reserves the decision whether to transfer data to an independent authority, as has been requested by data protection commissioners in the oral argument, is not necessary for safeguarding the fundamental right. What is lacking, however, is an obligation to keep a record of the transfer, as it is prescribed in the case of the execution of the monitoring and of the destruction and the deletion of the data. Under these circumstances, a sufficient control of the transfers by the panels established for that objective or a judicial review cannot take place. 280

The provisions cannot be interpreted to be in accord with the Constitution because, on the one hand, the parliament can remedy the unconstitutionality of the provisions in different ways. The Federal Constitutional Court must not anticipate such a solution. On the other hand, an interpretation of the provisions that is in accord with the Constitution would not be consistent with the requirement of specificity and clarity that the Basic Law places on provisions that permit the transfer of personal data obtained by an encroachment upon fundamental rights and the change of the objective for which this data may be used. The parliament is obliged to create consistency with the Basic Law. 281

VII.

§ 3.7 of the G 10 Act is inconsistent with Article 10 of the Basic Law. 282

Certainly, the regulation is, in itself, not objectionable from a constitutional point of view. When considered on its own, the regulation obliges the receiving agencies to evaluate whether they need the data transferred pursuant to § 3.5 of the G 10 Act for the objectives specified in § 3.3 of the G 10 Act. This is a step of selection that corresponds to the step regulated in § 3.4 of the G 10 Act. This step is meant to ensure, as established in §§ 3.3 and 3.5 of the G 10 Act, that the objective for which data is collected in a specific case is identified and that collecting data in this case is bound to this objective. Thus, it complies with the requirements of Article 10 of the Basic Law. Unlike § 3.4 of the G 10 Act, the provision in § 3.7(3) of the G 10 Act explicitly prohibits the further use of the data that is not needed but was not immediately destroyed 283

due to the unreasonable effort this would involve. Moreover, fundamental rights interests, especially that of the freedom of the press, can be sufficiently protected within the framework of the concept of necessity that is established in § 3.7(1) of the G 10 Act.

What is lacking, however, in this context as well as in the case of the corresponding powers of the Federal Intelligence Service, is the obligation to mark the data accordingly; the parliament is to impose this obligation on the receiving agencies as a safety precaution in the context of binding the use of data to a specific objective. Without such an obligation, the data and information from transfers pursuant to the G 10 Act could be stored, after being examined for their relevance as established in § 3.7 of the G 10 Act in such a way, or mix with other data and information, that their origin from a measure of strategic telecommunications monitoring is no longer recognisable. This would circumvent the restriction of use provided in § 3.3 of the G 10 Act. 284

An interpretation consistent with the constitution is ruled out in this case as well. The parliament is obliged to create consistency with the Basic Law. 285

VIII.

The provisions of § 3.8(2) of the G 10 Act, which address the duty to inform the subject of telecommunications monitoring that such monitoring has taken place, is not consistent with the Basic Law. 286

1. It is, however, not objectionable from the constitutional point of view that sentence § 3.8(1) of the G 10 Act only provides a restricted form of notice to the subject of telecommunications monitoring. Article 10.2(2) in conjunction with Article 19.4(3) of the Basic Law permits the withholding of such notice if the restriction of telecommunications privacy serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land* (Federal state). The jurisprudence of the Federal Constitutional Court, however, has established that this only applies when qualified by the limitation that the person affected is to be informed subsequently as soon as it can be precluded that the objective of the measure is jeopardised and a danger to the existence or security of the Federation or of a *Land* can be precluded as well (cf. BVerfGE 30, p. 1 [at pp. 31-32]). This leads to the conclusion that monitoring that serves the early recognition of the threat of an armed attack (§ 3.1[1] and § 3.1 sent. 2 no. 1 of the G 10 Act) is not objectionable from the constitutional point of view. 287

Certainly, these points of view do not apply to the threats added in nos. 2 to 6 of this regulation by the 1994 Fight against Crime Act. What applies in this context, however, is Article 10.2(1) of the Basic Law, which permits the restriction of telecommunications privacy for other objectives. Justification for such secrecy can include the risk that the disclosure of information or of methods applied, which are in the concrete case in question still to be kept secret, would jeopardise the fulfilment of the involved agency's mission (cf. BVerfGE 57, p. 250 [at p. 284]). Apart from the fulfilment of the involved agency's mission, overriding detriment to the good of the Federal Republic of Germany or to a *Land* (Federal state) that is to be expected if the affected person is informed, can, under certain circumstances, be taken into consideration as an opposing interest. In the intelligence service sector, this may be the case *e.g.* when foreign secret services are involved or in the field of counter-intelligence (in this context, see the decision of the *Oberverwaltungsgericht* [Higher Administrative Court] of Berlin, NVwZ [*Neue Zeitschrift für Verwaltungsrecht*] 1987, p. 817 [at p. 819]). The protection of informants can also be regarded as a legitimate interest that justifies the maintenance of secrecy (cf. BVerfGE 57, p. 250 [at p. 284]). 288

2. However, § 3.8(2) of the G 10 Act violates Article 10 and Article 19.4 of the Basic Law. 289

Pursuant to this regulation, notification of the measures restricting telecommunications privacy can be excused if the data has been destroyed by the Federal Intelligence Service or a receiving agency within three months after it was obtained. Thus, the regulation only focuses on the point in time when the data is deleted. For the decision whether or not to give notice to the subject of monitoring, it is not of importance what has happened to the data during the three-month period. As the oral argument 290

has shown, this results, in practice, in the monitored persons not being informed by the Federal Intelligence Service. Instead, the Federal Intelligence Service applies the regulation as if it established a duty to destroy data after three months.

Reasons of administrative practicability on which the regulation is based cannot justify such a far-reaching preclusion of the duty to give notice that telecommunications monitoring has taken place. It is true that, in view of the large number of screenings and in view of the fact that the material obtained largely proves irrelevant and is soon destroyed, there are legitimate reasons that justify withholding notification. The mere lapse of time, however, is not sufficient for justifying this, as it does not provide the assurance that within this period of time no further use has taken place. 291

As a general rule, it is the use to which collected data is put that constitutes the most grievous strain on a subject of telecommunications monitoring. Nonetheless, collecting the data itself constitutes an encroachment upon telecommunications privacy against which recourse to a court, in principle, must be possible. Under these circumstances, the fact that the affected person is not informed about the monitoring could, at most, be justified if the collected data was destroyed immediately, without further steps, as it was regarded as irrelevant. Without such a limitation, § 3.8(2) of the G 10 Act thus restricts Article 10 and Article 19.4 of the Basic Law in a disproportionate manner. 292

As the provision can be made consistent with the fundamental rights by amending it, it is not to be declared void but is only to be declared inconsistent with the Basic Law. The parliament is obliged to create consistency with the Basic Law. 293

IX.

However, the regulation on the preclusion of the recourse to a court in § 9.6 of the G 10 Act is consistent with the Basic Law. 294

This regulation has its constitutional basis in Article 10.2(2) of the Basic Law. This sentence permits, in the case of restrictions on telecommunications privacy that serve to protect the free democratic basic order or the existence or the security of the Federal Republic of Germany or of a *Land*, the preclusion of the right to the recourse to a court if that right is replaced by a review of the case by agencies and auxiliary agencies appointed by the parliament. The Federal Constitutional Court has declared this regulation, by which the 1968 constitutional amendment altered Article 10 of the Basic Law, consistent with Article 79.3 of the Basic Law (cf. BVerfGE 30, p. 1 [at pp. 26 *et seq.*]). 295

§ 9.6 of the G 10 Act keeps within the bounds of Article 10.2(2) of the Basic Law. The preclusion of the recourse to a court is limited to orders pursuant to § 2 and § 3.1 sent. 2 no. 1 of the G 10 Act and does not cover the threats specified in nos. 2-6 of this regulation. Parliamentary control is ensured by § 9 of the G 10 Act. Apart from that, the persons affected do have recourse to a court, pursuant to § 5.5(3) of the G 10 Act, after being informed of the measures restricting telecommunications priva- 296

cy. § 9.6 of the G 10 Act is declared to be inapplicable.

The question whether this also opens the recourse to a court in the cases of § 2 and § 3.1 sent. 2 no. 1 of the G 10 Act when the subjects of measures restricting telecommunications privacy have been informed is not important from the point of view of constitutional law. As regards the constitutional aspect, it is sufficient to state that when interpreting § 5.5(3) of the G 10 Act, notifying the monitored person may not be made the prerequisite of opening the recourse to a court. Even if the person affected has learned about the monitoring of his or her telecommunications traffic from another source, he or she is free to take recourse to a court. The possibility of taking recourse to a court would be unnecessarily diminished if the person affected by monitoring were also in such cases dependent on information about the monitoring activity being provided. 297

X.

The regulations on the deletion of data in § 3.6 and in §§ 3.7(2) and 3.7(3) as well as in § 7.4 of the G 10 Act are also consistent with the Basic Law. 298

They comply with the requirement, which follows from Article 10 of the Basic Law, that data obtained by means of encroachments upon telecommunications privacy be deleted as soon as it is no longer needed for the objectives that justify the encroachment. It cannot be inferred that the regulations fall short of the required minimum protection of fundamental rights. 299

Nor can the regulations be criticised from the perspective of Article 19.4 of the Basic Law. The guarantee of recourse to a court, however, prohibits measures that undermine the protection afforded by this guarantee (cf. BVerfGE 69, p. 1 [at p. 49]). The duty to delete data that is no longer required must therefore, for those cases in which a judicial review of telecommunications monitoring conducted by the Federal Intelligence Service is possible, be co-ordinated with the guarantee of recourse to a court in such a way that this guarantee is not circumvented. The provisions, however, permit such an interpretation. 300

§ 7.4(1) of the G 10 Act requires that data be deleted only if it is no longer of importance in the framework of the judicial examination of the legality of the measures that restrict telecommunications privacy. Pursuant to sent. 3 of the provision, this is to be evaluated every six months. As a general rule, this will mean that the data is to be stored for another six months after the person affected was informed about the monitoring. In this context, the interests of the monitored person are protected by §§ 7.4(4) and 7.4(5) of the G 10 Act, which require that the data is to be sealed, *i.e.* that it may only be used for the judicial examination. It can, *vice versa*, reasonably be expected of the monitored person that he or she decide within six months after being informed about the monitoring whether he or she wants judicial examination of the case. 301

XI.

The provision of § 9.2(3) of the G 10 Act, which provides for the control of the monitoring measures by the Commission, is inconsistent with Article 10 of the Basic Law. It does not sufficiently ensure that the control covers the entire process of screening and utilisation of the data. Without such control, the challenged regulations that contain authorisations could not continue to exist. It is true that § 9.2(3) of the G 10 Act provides that the Commission decides about the permissibility and necessity of measures restricting telecommunications privacy. It is not clear, however, what is to be understood by measures restricting telecommunications privacy. The subsequent provision of § 9.2(4) of the G 10 Act, according to which the responsible Federal Minister is to immediately cancel any orders which the Commission declares impermissible or unnecessary, could be interpreted to mean that the authorisation to control only refers to the ministerial order. 302

Such a view, which is incompatible with Article 10 of the Basic Law, is not only in the range of possibility. Rather, the Federal government expressed exactly such an interpretation in a letter to the G 10 Commission dated 9 December 1996. In spite of its diverging interpretation of the law, the Commission accepted this view and has since refrained from controlling in the cases of §§ 3.3, 3.5, 3.6 and § 3.8 of the G 10 Act. Due to the strict requirements placed on specificity when personal data is involved, the regulation therefore requires that the scope of its application be clarified. This clarification is to be made by the parliament. 303

Moreover it must be ensured that the G 10 Commission, in view of the fact that the Fight against Crime Act has considerably expanded the Federal Intelligence Service's monitoring activities, is provided with the staff needed to effectively fulfil its mission. Moreover, it must be ensured that sufficient control exists also in the administrative sector on the level of the *Länder* (Federal states) level, as far as the data obtained by eliminating telecommunication privacy is transferred to *Land* (Federal state) authorities pursuant § 3.5 of the G 10 Act. 304

XII.

To the extent that this judgement obliges the parliament to create consistency with the Basic Law, its time limit for doing so is 30 June 2001. 305

In the meantime, § 3.1 sent. 2 no. 5 of the G 10 Act may only be applied if counterfeiting committed abroad results in a threat to monetary stability in the Federal Republic of Germany. § 3.3(2) of the G 10 Act is to be applied with the limitation that the personal data contained in the Commission's report to the Federal government is marked and that it remains bound to the objectives that justified the collection of the data in the first place. § 3.4 of the G 10 Act is to be applied with the limitation that the personal data may be marked and may not be used for other objectives than those specified in § 3.1 of the G 10 Act. 306

§ 3.5(1) in conjunction with § 3.3(1) of the G 10 Act is applicable with the limitation 307

that personal data may only be transferred in accordance with the prerequisites of the temporary injunction order issued on 5 July 1995, and that a record of the transfer is kept. In this respect, the Federal Constitutional Court refrains from changing the present state of the law again only for the short transition period until a new regulation is enacted, although this means that in this transition period, the parts of the regulation that the parliament can enact again in the framework of a new regulation without violating the Basic Law may not be applied. If, on the contrary, the provision that has been declared unconstitutional were to remain applicable until the enactment of the new regulation, transfers of data would be possible that violate fundamental rights. In the oral argument, no evidence was provided that the temporary injunction order resulted in considerable detriment to the Federal Republic of Germany in the past. This aspect was the one that tipped the balance in the weighing of consequences. If the parliament regards the state of the law that is valid in the transition period as hardly tolerable, it is the duty of the parliament to change this state of the law by quickly enacting a new regulation.

§ 3.7 of the G 10 Act is to be applied with the limitation that the data must be marked. § 3.8(2) of the G 10 Act is applicable with the limitation that no utilisation of the data has taken place before it is deleted. § 9.2(3) of the G 10 Act is applicable with the limitation that the Commission's power to control also extends to measures pursuant to §§ 3.3, 3.5, 3.6 and 3.8 of the G 10 Act. 308

Papier Grimm Kühling

Jaeger Haas Hömig

Steiner

Bundesverfassungsgericht, Beschluss des Ersten Senats vom 14. Juli 1999 - 1 BvR 2226/94, 1 BvR 2437/95, 1 BvR 2420/95

Zitiervorschlag BVerfG, Beschluss des Ersten Senats vom 14. Juli 1999 - 1 BvR 2226/94, 1 BvR 2437/95, 1 BvR 2420/95 - Rn. (1 - 308), http://www.bverfg.de/e/rs19990714_1bvr222694en.html

ECLI ECLI:DE:BVerfG:1999:rs19990714.1bvr222694