Headnotes

to the Judgment 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 Basic Law not only provides protection against the state obtaining knowledge of telecommunications. It also protects against information and data processing measures that follow after the state permissibly obtained knowledge of such communications, and against any subsequent use of this data.**

2. **The territorial scope of protection under the privacy of telecommunications [guaranteed by Art. 10 of the Basic Law] is not limited to the domestic territory. Rather, Article 10 of the Basic Law may also be applicable if telecommunications that take place abroad are intercepted and analysed on domestic territory, which sufficiently links the interference to domestic state action.**

3. **Article 73 no. 1 of the Basic Law grants the Federation the competence to legislate on the interception, use and sharing of telecommunications data by the Federal Intelligence Service. However, Article 73 no. 1 of the Basic Law does not entitle the federal legislator to confer upon the Federal Intelligence Service powers that are aimed at the prevention or prosecution of criminal acts as such.**

4. **If the legislator authorises the Federal Intelligence Service to interfere with the privacy of telecommunications, Article 10 of the Basic Law requires that the legislator take precautions against the risks arising from the collection and use of personal data. These precautions include, in particular, that the use of the information obtained be limited to the purpose that justified the collection of the data in the first place.**

5. **The powers conferred upon the Federal Intelligence Service under § 1 and § 3 of the Article 10 Act to monitor, record and analyse telecommunications traffic data in order to ensure early detection of serious impending danger to the Federal Republic of Germany originating from abroad and to provide intelligence reports to the Federal Government is, in principle, compatible with Article 10 of the Basic Law.**

6. **The sharing of personal data obtained through telecommunications surveillance by the Federal Intelligence Service for its own purposes with other authorities is compatible with Article 10 of the Basic Law. It requires, however, that the data is necessary for achieving the purposes pursued by the receiving authority; that the requirements applicable to a change in purpose (BVerfGE 65, 1 <44 *et seq*., 62>) are met; and that the statutory thresholds for data sharing observe the principle of proportionality.**

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 2226/94 -

- 1 BvR 2420/95 -

- 1 BvR 2437/95 -

IN THE NAME OF THE PEOPLE

In the proceedings

on the constitutional complaints of

1. Prof. Dr. K...,

– authorised representative: …

against Article 1 § 3(1) first sentence and second sentence nos. 2 to 6, § 3(3), (4), (5), (7) and (8) of the Act of 13 August 1968 on Article 10 of the Basic Law (BGBl I, p. 949), in the version of the Fight Against Crime Act of 28 October 1994 (BGBl I, p. 3186), as amended by the Act of 17 December 1997 (BGBl I, p. 3108),

-1 BvR 2226/94 -,

2. a) Dr. W…, b) Mr S...,

– authorised representative: …

against Article 1 § 1(1), § 3(1), (2) third sentence, § 3(3) to (8), § 7(4), § 9(6) of the Act of 13 August 1968 on Article 10 of the Basic Law (BGBl I, p. 949) in the version of the Fight Against Crime Act of 28 October 1994 (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: …

against Article 1 § 3(1) first sentence and second sentence nos. 2 to 6, § 3(2) to (8) of the Act of 13 August 1968 on Article 10 of the Basic Law (BGBl I, p. 949) in the version of the Fight Against Crime Act of 28 October 1994 (BGBl I, p. 3186), as amended by the Act of 17 December 1997 (BGBl I, p. 3108),

- 1 BvR 2437/95 -

the Federal Constitutional Court – First Senate –

with the participation of Justices

Vice-President Papier

Grimm,

Kühling,

Jaeger,

Haas,

Hömig,

Steiner

held on the basis of the oral hearing of 15 and 16 December 1998:

JUDGMENT

1. **§ 3(1) first sentence and second sentence no. 5, § 3(3), (4), (5) first sentence, (7) first sentence, (8) second sentence, and § 9(2) third sentence of the Act on Article 10 of the Basic Law (the Act) revised by the Fight Against Crime Act of 28 October 1994 (BGBl I, p. 3186), as amended by the Accompanying Act to the Telecommunications Act of 17 December 1997 (BGBl I, p. 3108), are incompatible with Article 10 of the Basic Law. Moreover, § 3(3) first sentence, (4) and (5) first sentence of the Act is incompatible with Article 5(1) second sentence of the Basic Law, and § 3(8) second sentence of the Act is incompatible with Article 19(4) of the Basic Law.**
2. **For the rest, the constitutional complaints of complainants nos. 1, 2a and 3 are rejected.**
3. **The constitutional complaint of complainant no. 2b is dismissed as inadmissible.**
4. **[…]**

REASONS:

A.

The constitutional complaints concern the powers of the Federal Intelligence Service (*Bundesnachrichtendienst*) to monitor, record and analyse telecommunications traffic and to share the data thus obtained with other authorities. The constitutional complaints also challenge other provisions of the Act on Article 10 of the Basic Law 1

*(*hereinafter: the Act*)* as amended in 1994 by the Fight Against Crime Act.

I.

1. In its original version, the Act […] already provided for the possibility of telecommunications surveillance (§ 1 of the Act). Surveillance was permissible in two forms. § 2 of the Act governed the gathering of intelligence on individual persons. According to this provision, surveillance of individuals was permissible if there were grounds for suspecting that someone was planning, committing or had committed certain particularly serious criminal offences that threatened the existence of the Federal Republic of Germany or its democratic order. § 3 of the Act governed so-called strategic surveillance, which served in particular to obtain situation reports on certain impending dangers *(drohende Gefahren)* to the Federal Republic of Germany. 2

The proceedings at hand only concern strategic surveillance. Pursuant to § 3(1) second sentence of the Act (former version), strategic surveillance was originally only permissible to ensure early detection of a danger of armed attacks against the Federal Republic of Germany, and to avert such dangers. […] 3

An essential feature of the measures restricting the privacy of telecommunications pursuant to § 3 of the Act (former version) was that they did not specifically target individual persons, which in any case would not have been technologically feasible at that time, but served to obtain non-person-related intelligence to provide the Federal Government with information concerning matters of foreign and defence policy. […] 4

[…] 5

2. The […] Fight Against Crime Act of 28 October 1994 (BGBl I, p. 3186) provided for several amendments to the Act. […] 6

The amendments expanded the purposes that could constitute grounds for surveillance measures pursuant to § 3(1) second sentence of the Act. In addition to the danger of armed attacks (no. 1), the amendments added five further categories of danger situations arising from different forms of criminal conduct with an international dimension. These categories were as follows: international terrorist attacks (no. 2), international proliferation of military weapons and trading of 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 activities set forth under nos. 3 to 5 (no. 6). 7

Yet, as regards these newly added statutory purposes of intelligence operations carried out under the Act, surveillance is limited to wireless international telecommunications traffic (§ 3(1) first sentence of the Act), for which the necessary technology did not yet exist at the time the original Act was enacted. Wired telecommunications may only be intercepted if there is danger of a war of aggression (§ 3(1) third sentence of the Act). The geographic reach of surveillance was also expanded by the newly introduced categories of relevant dangers under nos. 2 to 6 of the provision. 8

[…]

Moreover, the amendments expanded the scope of the Act in terms of persons that could be targeted by surveillance. It is true that § 3(2) second sentence of the Act does not allow the targeted interception of specific subscriber lines. Pursuant to § 3(2) first sentence of the Act, subscriber lines are selected for surveillance on the basis of search terms that must serve the gathering of intelligence on the danger situations specified in the warrant [authorising the measure], and which must be suitable for achieving this purpose. However, according to the third sentence of the provision, this does not apply with regard to individual subscriber lines belonging to foreigners in other countries. Their subscriber numbers may [directly] be used as so-called formal search terms. In practice, the number of persons targeted in this manner is much higher today because now – unlike in the past – the technological means exist that make it generally possible to identify the individual subscriber lines involved in telecommunications. 9

[…] 10-11

§ 1(1) of the Act provides the general statutory basis for the powers conferred upon the Federal Intelligence Service to intercept and record telecommunications. […] 12

[…] 13-40

§ 7(4) of the Act governs the destruction of personal data obtained by the measures set forth under § 2 and § 3 of the Act; § 9 of the Act sets out an oversight mechanism while excluding recourse to the courts. […] 41

[…] 42-46

3. […] 47

4. […] 48

II.

1. With his constitutional complaint, complainant no. 1 challenges the expansion of the Federal Intelligence Service's powers to interfere with fundamental rights as provided for in § 3(1) second sentence nos. 2 to 6 of the Act; he also challenges the statutory design of the notification requirements in § 3(8) of the Act. […] 49

[…] 50-63

2. Complainants nos. 2a and 2b additionally challenge the strategic surveillance powers laid down in § 1(1), § 3(1) first sentence, second sentence no. 1 and third sentence of the Act; the envisaged destruction of obtained data without the consent of the affected persons pursuant to § 3(6) and (7) second and third sentence, § 7(4) of the Act; and the exclusion of recourse to the courts set forth in § 9(6) of the Act. […] 64

[…] 65-74

3. Complainants no. 3 challenge § 3(1) first sentence and second sentence nos. 2 to 6 and § 3(2) to (8) of the Act, claiming that these provisions violate the Basic Law, specifically Art. 10, Art. 2(1) in conjunction with Art. 1(1), Art. 5(1) second sentence, Art. 19(4), Art. 20(2) and Art. 73 nos. 1 and 10 of the Basic Law. 75

[…] 76-82

III.

Statements in the constitutional complaint proceedings were submitted by the Federal Minister of the Interior on behalf of the Federal Government, the Government of the Free State of Bavaria, the Federal Data Protection Officer and the data protection officers of the *Länder* Bavaria, Berlin, Brandenburg, Bremen, Hamburg, North Rhine-Westphalia, Saarland and Schleswig-Holstein. 83

[…] 84-141

IV.

[…] 142

B.

With the exception of the constitutional complaint lodged by complainant no. 2b, the constitutional complaints are admissible. 143

[…] 144-156

C.

The challenged provisions are not fully compatible with the Basic Law. 157

I.

The standard of review regarding the constitutionality of the challenged provisions derives primarily from Art. 10 of the Basic Law. The right to informational self-determination that follows from Art. 2(1) in conjunction with Art. 1(1) of the Basic Law is not applicable in addition to Art. 10 of the Basic Law since, in the context of telecommunications, Art. 10 of the Basic Law contains a more specific guarantee that supersedes the aforementioned general guarantee (cf. BVerfGE 67, 157 <171>). In addition, Art. 19(4) of the Basic Law is affected regarding the possibility of recourse to the courts against measures taken pursuant to § 3 of the Act and the restrictions of legal recourse pursuant to § 9(6) of the Act. Moreover, the constitutional complaints lodged by complainants nos. 2a and 3 must be measured against Art. 5(1) second sentence of the Basic Law. 158

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

a) The privacy of telecommunications primarily covers the contents of communications. The state should, in principle, not be allowed to obtain knowledge of the contents of information and thoughts exchanged, orally or in writing, via telecommunications systems. In this context, Art. 10 of the Basic Law does not distinguish between communication of a private nature and other communication, e.g. business or political communication (cf. BVerfGE 67, 157 <172>). Rather, the fundamental rights protection extends to all communication taking place by means of telecommunications technology. 160

Yet the fundamental rights protection is not limited to shielding the actual communication contents against the state obtaining knowledge thereof. It also extends to the circumstances of a communication, which include whether, when and how often telecommunications traffic occurred or was attempted between whom or between which devices (cf. BVerfGE 67, 157 < 172>; 85, 386 <396>). The state is generally not entitled to obtain knowledge of these circumstances. The confidential use of the telecommunication medium must be ensured in all respects. 161

By generally shielding individual communications from the reach of the state, the fundamental right is meant to preserve the conditions that are necessary to ensure free telecommunications in general. The inviolability of telecommunications privacy, as guaranteed by fundamental rights, seeks to prevent a situation where communication participants have to expect that state authorities will intercept their communications and obtain knowledge of the relevant communication relations or contents, as a result of which affected persons might cease to exchange opinions or information by means of telecommunications systems altogether, or change how and what they communicate. 162

In addition, the freedom of telecommunications that Art. 10 of the Basic Law safeguards is adversely affected if there is reason to fear that the state will use the knowledge of telecommunications circumstances and contents to the detriment of the communication partners in other contexts (for an overview cf. BVerfGE 65, 1 <42 and 43>; 93, 181 <188>). For these reasons, the protection afforded by Art. 10 of the Basic Law applies not only to the state obtaining knowledge of telecommunications that the communication partners wish to keep to themselves, but also to the information and data processing measures that follow after the state has obtained knowledge of protected communications, and to the use of this data (regarding the right to informational self-determination, cf. already BVerfGE 65, 1 <46>). 163

b) Art. 10(2) of the Basic Law does permit restrictions of telecommunications privacy. However, such restrictions not only require, like any other fundamental rights restriction, a statutory basis that serves a legitimate purpose in the interest of the common good and satisfies the principle of proportionality for the rest. Art. 10 of the Basic Law also imposes on the legislator particular requirements that are specific to the processing of personal data obtained through interferences with telecommunications 164

privacy. In this respect, the requirements that the Federal Constitutional Court derived from Art. 2(1) in conjunction with Art. 1(1) of the Basic Law in its *Census* decision (cf. BVerfGE 65, 1 <44 *et seq*.>) can largely be applied accordingly to the more specific guarantee of Art. 10 of the Basic Law, too.

This includes that the prerequisites and scope of restrictions be clearly set out in the statutory framework so that they are foreseeable for the individual. In particular, the statutory purposes for which interferences with telecommunications privacy are permissible must be specified precisely for each subject matter. Furthermore, the data collected must be suitable and necessary for achieving these purposes. The gathering and retention of data that has not been rendered anonymous for undefined or yet to be defined purposes would not be compatible with these requirements. Therefore, the storage and use of obtained data is, in principle, only permissible for a purpose specified in the law that authorises state authorities to obtain knowledge of the data. 165

The data does not lose the confidentiality protection afforded by Art. 10 of the Basic Law because a state authority has already obtained knowledge of the telecommunications in question; therefore, the requirements deriving from this fundamental right also apply to the subsequent sharing of data and information that was obtained by measures setting aside the privacy of telecommunications. This holds true all the more as the sharing of data typically not only expands the groups of bodies or persons who have knowledge of the communication but also means that the data becomes available for uses in other contexts; this gives rise to additional, possibly more serious consequences for the affected persons than the original context in which their data was used. 166

The principle of purpose limitation does not preclude changes in purpose [regarding data use] altogether. However, such changes require a separate statutory basis that is formally and substantively compatible with the Basic Law. This means, *inter alia*, that a change in purpose must be justified by public interests that outweigh the interests protected by the affected fundamental rights. The new purpose must be related to the responsibilities and powers of the authority with which the data is shared, and it must be set out in sufficiently clear statutory provisions. Moreover, the new purpose must not be incompatible with the primary purpose for which the data was originally collected (cf. BVerfGE 65, 1 <51, 62>). 167

The required purpose limitation can only be guaranteed if the obtained data subsequently remains identifiable as data stemming from an interference with telecommunications privacy. Therefore, constitutional law requires that the data be labelled accordingly. 168

Moreover, under Art. 10 of the Basic Law the holders of fundamental rights are entitled to be notified of measures of telecommunications surveillance affecting them. This is necessary to ensure effective fundamental rights protection, given that without this information, the affected persons can neither challenge the lawfulness of the interception and monitoring of their telecommunications, nor assert possible rights to 169

have their data deleted or rectified. This right is not necessarily limited to ensuring recourse to the courts under Art. 19(4) of the Basic Law. Rather, it is a specific right to data protection that can be asserted vis-à-vis the authority that processes the relevant information and data.

[…] To the extent that the purpose pursued by the measure interfering with the privacy of telecommunications would be frustrated if the affected person were notified, it is not objectionable under constitutional law to limit the notification requirement where necessary. It may be sufficient to only inform the person concerned about the interference at a later stage (cf. BVerfGE 49, 329 <342 and 343>). 170

Affected persons can neither perceive interferences with the privacy of telecommunications nor the subsequent data processing; moreover, the possibility of limiting the notification requirement leads to gaps in legal protection. For these reasons, Art. 10 of the Basic Law requires oversight by state bodies and auxiliary bodies that are independent and not bound by instructions (cf. BVerfGE 30, 1 <23 and 24, 30 and 31>; 65, 1 <46>; 67, 157 <185>). Yet the Constitution does not specify the details of the oversight regime. The legislator is free to choose the mechanisms it regards as the most suitable as long as the oversight regime is sufficiently effective. To be effective, oversight must extend to all stages of the surveillance process. Oversight mechanisms must assess both whether the interference with telecommunications privacy is lawful and whether legal safeguards protecting telecommunications privacy are adhered to. 171

Finally, given that the interception and recording of telecommunications traffic and the use of the information obtained is limited to specific purposes, the data must be destroyed as soon as it is no longer needed for achieving the specified purposes nor for allowing recourse to the courts. 172

c) The territorial scope of protection under Art. 10 of the Basic Law has not yet been determined in the case-law of the Federal Constitutional Court. […] 173

Art. 1(3) of the Basic Law defines the general scope of application of fundamental rights and thus provides the basis for determining the territorial scope of Art. 10 of the Basic Law. Under Art. 1(3) of the Basic Law, the legislature, the executive and the judiciary are strictly bound by fundamental rights. However, this constitutional provision does not exhaustively determine the reach of fundamental rights in terms of territorial protection. The Basic Law is not limited to defining the domestic order of the German state, but also determines the essential elements of its relationship with the international community. In this respect, the Basic Law is informed by the necessity to seek a delimitation from and coordination with other states and legal systems. On the one hand, the scope of the competences and responsibilities incumbent upon German state organs must be taken into account when determining the binding effect of fundamental rights (cf. BVerfGE 66, 39 <57 *et seq*.>; 92, 26 <47>). On the other hand, constitutional law must be reconciled with international law. Yet international law does not *per se* rule out that fundamental rights are applicable in matters that 174

have a foreign dimension. Rather, the scope of fundamental rights must be derived from the Basic Law itself, taking into account Art. 25 of the Basic Law. Depending on the constitutional guarantee in question, further modifications and differentiations may be permissible or required (cf. BVerfGE 31, 58 <72 *et seq*.>; 92, 26 <41 and 42>).

The protection of telecommunications privacy afforded by Art. 10 of the Basic Law seeks to ensure – in line with international law (cf. Art. 12 of the Universal Declaration of Human Rights of 10 December 1948; Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950; in this regard ECtHR, *Klaas and Others v. Germany*, Judgment of 6 September 1978, no. 5029/71, NJW 1979, p. 1755 <1756>) – that telecommunications remain free of unwanted or unnoticed surveillance and that the holders of fundamental rights can communicate without worry or fear. The protection of telecommunications privacy is tied to the use of a communication medium and aims to counteract the risks to confidentiality that specifically result from the use of such a medium, which makes telecommunications more vulnerable to state interference than direct communication between persons who are physically present (cf. BVerfGE 85, 386 <396>). Modern technology, like satellite and radio transmission, permits access to foreign telecommunications traffic, too, by means of surveillance equipment that is located on the territory of the Federal Republic of Germany. 175

The interception and recording of telecommunications traffic with receiving equipment of the Federal Intelligence Service that is located on German territory already establishes a technical and informational connection to the respective communication participants and a connection – characterised by the unique nature of data and information – to German territory. Moreover, the analysis of telecommunications thus intercepted is carried out by the Federal Intelligence Service on German territory. These circumstances create a link between the communication undertaken abroad and state action carried out on domestic territory that subjects the latter to the binding effect of Art. 10 of the Basic Law even if one were to assume that a sufficient territorial link was required in this regard. In the case at hand, it is not necessary to decide on intelligence service activities other than the ones governed by the challenged provisions nor on what applies to foreigners participating in telecommunications abroad. […] 176

2. In part, the challenged provisions must also be measured against Art. 19(4) of the Basic Law. 177

Art. 19(4) of the Basic Law guarantees everyone the right to effective judicial review in the event of a possible violation of their rights by acts of public authority. However, Art. 19(4) third sentence of the Basic Law states that this applies without prejudice to Art. 10(2) second sentence of the Basic Law, which specifically exempts interferences with the privacy of telecommunications from the otherwise comprehensive guarantee of legal protection. Yet these provisions do not exempt such interferences 178

from any review whatsoever. Rather, the lack of recourse to the courts must be compensated by a review carried out by bodies and auxiliary bodies appointed by Parliament.

Furthermore, the right afforded by Art. 19(4) of the Basic Law is not limited to judicial review and judicial proceedings. As the guarantee of legal protection aims to safeguard the effective exercise of other, substantive rights, it may require that a person under surveillance be notified of the surveillance measures if notification is a necessary precondition for seeking recourse to the courts (cf. BVerfGE 65, 1 <70>), including in cases where Art. 10 of the Basic Law is applicable. However, Art. 19(4) of the Basic Law does not rule out restrictions of this right, and in any case requires statutory provisions that specify the details of such restrictions. 179

The obligation to ensure that data be in principle destroyed when it is no longer needed must also be read in light of Art. 19(4) of the Basic Law. The guarantee of legal protection under Art. 19(4) of the Basic Law prohibits measures that aim to frustrate legal protection of the affected persons, or are likely to do so (cf. BVerfGE 69, 1 <49>). In cases in which affected persons seek judicial review of information and data processing measures by the state, the obligation to destroy data must be balanced against the guarantee of legal protection so as to ensure that legal protection is not undermined or frustrated. 180

3. […] 181-183

II.

The challenged provisions allow for interferences with the above-mentioned fundamental rights in several respects. 184

1. The surveillance and recording of wireless international telecommunications by the Federal Intelligence Service interferes with the privacy of telecommunications. 185

Given that Art. 10(1) of the Basic Law serves to protect the confidentiality of communications, any instance where the state obtains knowledge of, records or processes communication data constitutes an interference with fundamental rights (cf. BVerfGE 85, 386 <398>). […]. 186

This means that the interception itself already constitutes an interference, to the extent that it makes the intercepted communication available to the Federal Intelligence Service and is the basis for the subsequent cross-checking with search terms. […] 187

The interference is perpetuated when the intercepted data is stored, which allows the data material to be accessed for cross-checking with search terms. The cross-checking itself again amounts to an additional interference as it determines the selection of data for further analysis. […] 188

The examination required under § 3(4) of the Act to determine whether the personal data obtained through telecommunications surveillance is necessary for achieving 189

the legitimate purposes pursued also constitutes an interference. This examination involves a deliberate selection of data, as the recorded data is either cleared for further processing or for storage to allow for future uses, or it is destroyed.

When the Federal Intelligence Service, in the context of its obligation to report to the Federal Government, shares personal data obtained through telecommunications surveillance, this also amounts to an interference since it expands the group of those who have knowledge of the relevant communications and can make use of this information. The transfer of data by the Federal Intelligence Service to the receiving authorities pursuant to § 3(5) and § 3(3) of the Act, and the examination of the data by the receiving authorities pursuant to § 3(7) of the Act, likewise amount to interferences. 190

The exemptions from the requirement to notify persons under surveillance of the measures restricting their telecommunications privacy pursuant to § 3(8) first and second sentence of the Act also amounts to an impairment of the privacy of telecommunications. 191

2. Moreover, the statutory exemptions from the requirement to notify persons under surveillance pursuant to § 3(8) first and second sentence, and the exclusion of recourse to the courts pursuant to § 9(6) of the Act, impair the guarantee of legal protection under Art. 19(4) of the Basic Law. In addition, the obligation to destroy personal data pursuant to § 3(6), § 3(7) and § 7(4) of the Act can adversely affect the possibilities of judicial review with regard to the measures. 192

3. […] 193

III.

The powers to monitor and record telecommunications traffic pursuant to § 1(1) and § 3(1) second sentence nos. 1 to 6 of the Act are for the most part compatible with Art. 10 of the Basic Law. However, § 3(1) second sentence no. 5 of the Act is incompatible with this fundamental right to the extent that the provision permits surveillance measures for the purposes of gathering intelligence for the timely detection of counterfeiting committed abroad and for counteracting such counterfeiting. 194

1. Formally, § 1(1) and § 3(1) of the Act do not raise constitutional concerns. The Federation has legislative competence for the subject matters governed by these provisions. This follows from Art. 73 no. 1 of the Basic Law, which confers exclusive legislative competence on the Federation in foreign affairs and defence matters. 195

[…] 196-206

2. § 1(1) and § 3(1) of the Act also satisfy the requirements of specificity and legal clarity deriving from Art. 10 of the Basic Law when conferring statutory powers to interfere with telecommunications. 207

[…] 208

3. Substantively, § 3(1) second sentence no. 5 of the Act disproportionately restricts telecommunications privacy. For the rest, § 3(1) second sentence of the Act satisfies the requirements deriving from the principle of proportionality. 209

a) The purpose of ensuring the timely detection of the dangers listed in nos. 1 to 6 of the provision, and of counteracting them, is a legitimate interest of the common good. It is true that the categories of dangers listed in nos. 2 to 6, which were newly added to the Act, do not carry the same weight as the danger of an armed attack, which has been recognised as legitimate grounds for telecommunications surveillance from the outset (cf. BVerfGE 67, 157 <178>). […] However, they do concern, albeit to differing degrees, high-ranking interests of the common good, the violation of which would result in serious harm to external and domestic peace and to protected legal interests of individuals. 210

b) Surveillance of telecommunications on the basis of § 3(1) of the Act is suitable for achieving the purpose of the law. 211

Its suitability is not called into question merely because the method of data collection indiscriminately affects a large number of persons yet only yields useful intelligence in comparatively few cases. At the legislative level, it is sufficient that there is an abstract possibility of achieving the intended purpose, i.e. that the measures are not unsuitable from the outset but may be conducive to the desired outcome (cf. BVerfGE 90, 145 <172>). This is the case here. 212

The requirement of suitability is also sufficiently reflected at the level of implementation. […] 213

[…] 214-216

c) The Act is necessary for achieving the purpose pursued. No other means are available that would be equally effective but less intrusive for fundamental rights holders. […] 217

d) The restrictions of the privacy of telecommunications traffic under § 1(1) and § 3(1) of the Act (intercepting, recording, storing, cross-checking) are for the most part proportionate in the strict sense. Only the restriction of telecommunications privacy for the purposes of detecting counterfeiting committed abroad (no. 5) fails to meet this requirement. 218

aa) The principle of proportionality requires that the curtailing of freedom protected by fundamental rights not be disproportionate to the purposes of the common good that the restriction of fundamental rights aims to achieve. Given that the individual is connected to and bound by the community, they must accept that fundamental rights are subject to restrictions serving overriding public interests (cf., e.g., BVerfGE 65, 1 <44>, with further references). However, the legislator must strike an appropriate balance between public interests and the interests of the individual. With respect to the fundamental rights interests, it must be taken into account which and how many hold- 219

ers of fundamental rights are affected by impairments, how intense these impairments are, and on what basis they occur. Thus, relevant criteria include the design of the statutory thresholds for carrying out the measures constituting interferences, the number of persons affected, and the severity of the impairments. This, in turn, depends on whether the communication participants remain anonymous; on what type of conversations and communication contents can be intercepted (cf., e.g., on the standard deriving from Art. 2(1) in conjunction with Art. 1(1) of the Basic Law, BVerfGE 34, 238 <247>); and on the disadvantages the holders of fundamental rights might face or have reason to fear on account of the surveillance measures. With respect to the interests of the common good, the weight of the underlying aims and interests that the surveillance measures serve must be determined. This depends, *inter alia,* on the scale and likelihood of the dangers that the surveillance measures aim to detect.

bb) The challenged provisions seriously impair the privacy of telecommunications. 220

Nonetheless, complainant no. 1 errs in claiming that the legislator completely abolished telecommunications privacy protected by Art. 10 of the Basic Law, infringing upon the essence (*Wesensgehalt*) of the fundamental right within the meaning of Art. 19(2) of the Basic Law. The provisions neither allow “global and sweeping surveillance”, which would be prohibited by the Basic Law even for gathering foreign intelligence (cf. BVerfGE 67, 157 <174>), nor do they allow the unconditional interception of all telecommunications of individual fundamental rights holders. Rather, surveillance and recording of telecommunications traffic remain subject to legal and factual limitations. 221

[…] 222-230

In determining the intensity of the fundamental right impairments, it must be taken into account that anyone participating in international telecommunications is exposed to the surveillance measures, regardless of whether their conduct has any connection to the surveillance or prompted it. In terms of content, the surveillance extends to any kind of communication in its entirety. Therefore, it cannot be ruled out that staff of the Federal Intelligence Service will obtain knowledge thereof. […] 231

[…] 232

In respect of the intensity of the fundamental right impairments at issue, the lack of anonymity regarding the communication participants must be taken into account as well. The linking of gathered intelligence to specific individuals is not limited to the interception and recording stage only, but in practice continues thereafter. […] 233

The disadvantages that are to be objectively expected or feared [by affected persons] may materialise as soon as the state obtains knowledge of the communication. Even before such knowledge is obtained, the fear of being under surveillance and the risk that communications may be recorded, subsequently analysed, and then possibly shared with and further used by other authorities, may lead to communication be- 234

ing no longer free from fear or worry, to communication disruptions and to changes in communication behaviour, in particular because the communicating parties avoid certain conversation topics or terms. The covert surveillance of telecommunications not only entails individual impairments for a large number of fundamental rights holders, but affects communication in society as a whole. In respect of the right to informational self-determination, which is comparable in this respect, the Federal Constitutional Court has therefore recognised a dimension of this right that serves the common good, going beyond the interest of the individual (cf. BVerfGE 65, 1 <43>).

cc) However, it is significant that the fundamental rights restrictions at issue serve to protect high-ranking interests of the common good. 235

Surveillance measures under § 3(1) first sentence and second sentence no. 1 of the Act are intended to yield intelligence about facts that are relevant for national defence in order to ensure timely detection if the Federal Republic of Germany is in danger of an armed attack. […] 236

The proliferation of international organised crime, in particular the illegal trading of military weapons and narcotics as well as money laundering, have resulted in increased dangers in the new fields of surveillance recognised in the challenged provisions. […] 237

These dangers, which all have in common that they originate abroad and which the powers conferred aim to detect, carry significant weight. The same applies to the danger of armed attacks but also, as has been sufficiently demonstrated by the Federal Intelligence Service, to the dangers of weapons proliferation, arms trading and international terrorism. […] 238

dd) Based on a balancing of interests that takes these aspects into consideration, § 3(1) second sentence nos. 1 to 4 and no. 6 of the Act are not objectionable under constitutional law. 239

Contrary to the opinion of complainant no. 1, the powers to monitor and record communications and the other measures provided for in the challenged provisions are not disproportionate from the outset because the exercise of these powers is not subject to specific thresholds, such as a specific danger (*konkrete Gefahr)* as traditionally required for public security measures, or sufficient grounds for the suspicion of criminal conduct *(hinreichender Tatverdacht)* as required in the context of law enforcement. The surveillance of telecommunications under the Act is indeed not based on any grounds for suspicion. In this regard, the interference with fundamental rights is not merely limited to the general risk that affected persons might be falsely suspected of wrongdoing. Rather, anyone could easily become the object of surveillance in the course of the measures authorised and carried out under the Act. 240

However, the purposes pursued by the Act differ [from traditional public security and law enforcement purposes]; therefore, it is justified that the statutory prerequisites for interferences with the privacy of telecommunications under the Act are of a different 241

design than those set out in police law [on public security] or the law of criminal procedure. Given that the federal legislative competence for the Act follows from Art. 73 no. 1 of the Basic Law, the purpose of surveillance measures carried out by the Federal Intelligence Service is from the outset limited to gathering foreign intelligence with respect to certain danger situations in the fields of foreign and security policy. […]

Under constitutional law, even the significant dangers that the telecommunications surveillance measures at issue aim to counter would not justify surveillance powers for the purposes of gathering foreign intelligence if such powers were not subject to any prerequisites or limitations. Yet the legislator actually made sure to specify such prerequisites. The Act does set out certain substantive criteria and procedural safeguards in the first and second sentence of its § 3(1). Substantively, the provision states in particular that intelligence may only be gathered if knowledge of the investigated situation is necessary to ensure the timely detection of dangers. Procedurally, the issuance by the competent ministry of a warrant directing and authorising the surveillance measure requires that the Federal Intelligence Service comprehensively establish, in its application for the warrant, why the targeted telecommunications relations could provide timely information about relevant dangers. 242

Taking into account the safeguards provided for in the Act, the envisaged interception and recording for the purpose of providing intelligence reports to the Federal Government do not appear disproportionate. While the number of intercepted telecommunications relations is far from negligible, it is still relatively low when seen in relation to the total volume of telecommunications, or even just the total volume of relevant international telecommunications. In this respect, it is particularly important that § 3(2) second sentence of the Act prohibits the targeted surveillance of specific individual subscriber lines. Without this prohibition, the principle of proportionality would not be satisfied, given that the surveillance powers do not require any grounds for suspicion, provide for the interception of a large number of telecommunications, and allow for the possibility of identifying the communication participants. […] It is true that the interception and recording of telecommunications as such could already hamper free communication, which Art. 10 of the Basic Law aims to protect; yet the full extent of this risk only materialises in the subsequent analysis and especially the sharing of intelligence thus obtained. In this respect, however, the risk to fundamental rights can be sufficiently counteracted by the design of the statutory powers concerning data analysis and sharing. 243

ee) Nevertheless, § 3(1) second sentence no. 5 of the Act, which sets out the danger of counterfeiting committed abroad [as possible grounds for surveillance], does not satisfy the principle of proportionality in its strict sense. 244

Counterfeiting neither poses a danger that is as serious as the danger of an armed attack, nor does it concern legal interests that are as significant as those affected by the other categories of dangers added to § 3 of the Act by the 1994 Fight Against 245

Crime Act. Nor do the various forms of counterfeiting give rise to the same level of potential danger that characterises the other listed grounds for interference. […]

§ 3(1) second sentence no. 5 of the Act could be rendered compatible with the Basic Law if certain limitations were incorporated into the provision. It is therefore not declared void, but only incompatible with the Basic Law. It is incumbent upon the legislator to bring the law in conformity with the Constitution. 246

IV.

§ 3(4) of the Act, which requires the Federal Intelligence Service to assess whether the personal data obtained through telecommunications surveillance is necessary for achieving the purposes invoked to justify the measures, is not as such objectionable under constitutional law. It does, however, not sufficiently give effect to the requirement of a purpose limitation, which derives from Art. 10 of the Basic Law, nor to the prohibition of excessive measures (*Übermaßverbot*). In this respect, the provision is incompatible not only with the privacy of telecommunications but also with freedom of the press, which must be taken into account as well. 247

This notwithstanding, § 3(4) of the Act does satisfy the principle of purpose limitation to the extent that this provision requires that the Federal Intelligence Service assess whether the data obtained through the surveillance of telecommunications is suitable for achieving the specified purpose. Moreover, § 3(6) first sentence of the Act reflects the principle of purpose limitation in that it prescribes that data be destroyed or deleted if its examination has shown that the data is not needed for the purposes pursued by the Federal Intelligence Service. However, the Act does not sufficiently guarantee that the use of data which is not destroyed or deleted remains limited to the purpose that justified its collection in the first place. The Act does not exclude possible data uses that go beyond the early detection of the dangers listed in the Act and the corresponding intelligence reports provided to the Federal Government. […] In addition, § 3(4) of the Act does not give effect to the requirement of labelling the data [as stemming from interferences with telecommunications privacy], which follows from Art. 10 of the Basic Law; without such labelling, it is no longer possible to identify the data that enjoys the fundamental rights protection afforded by Art. 10 of the Basic Law during later stages of data processing. 248

Furthermore, the challenged provision does not subject further data analysis to a statutory threshold, as would be required under the prohibition of excessive measures. § 3(3) of the Act, which subjects use of the data to specific requirements, does not apply to the Federal Intelligence Service itself. Instead, the provision concerns use of the data for the purposes of preventing, investigating or prosecuting criminal acts and thus [only] concerns the authorities with whom the Federal Intelligence Service is obliged to share intelligence pursuant to § 3(5) of the Act. The Act does not contain provisions ensuring that the Federal Intelligence Service itself may only analyse data stemming from telecommunications surveillance if the data is sufficient- 249

ly relevant to the dangers listed in § 1(1) and 3(1) of the Act. The lack of such a statutory threshold is also significant with regard to Article 5(1) second sentence of the Basic Law because this threshold would ensure that the Federal Intelligence Service takes into account the particularly weighty interests of protecting informants and journalistic confidentiality.

It is not possible to interpret the provision in conformity with the Constitution as this would run counter to the requirements of legal clarity and specificity deriving from Art. 10 of the Basic Law. However, as statutory amendments could remedy the constitutional shortcomings of the challenged provision, it is not declared void, but only incompatible with the Basic Law. It is incumbent upon the legislator to bring the law in conformity with the Constitution. 250

V.

The Federal Intelligence Service's obligation to report to the Federal Government under § 12 of the Federal Intelligence Service Act is only challenged in these proceedings to the extent that, pursuant to § 3(3) second sentence of the Act, this obligation is exempt from the limitations set out in § 3(3) first sentence of the Act. In this respect, the statutory framework lacks sufficient safeguards for protecting the privacy of telecommunications. 251

Art. 10 of the Basic Law (and Art. 5(1) of the Basic Law to the extent that communication protected by freedom of the press is concerned) also applies to the Federal Intelligence Service's obligation to provide intelligence reports to the Federal Government given that these reporting obligations are one of the purposes for which the Federal Intelligence Service was granted powers to carry out telecommunications surveillance. […]. 252

It is not objectionable that § 3(3) second sentence of the Act exempts the reporting obligation under § 12 of the Federal Intelligence Service Act from the limitations on data use pursuant to § 3(3) first sentence of the Act, as the limitations set out in this provision are not suited to the tasks of the Federal Intelligence Service. However, it is incompatible with Art. 10 of the Basic Law that the Federal Intelligence Service is not even subject to the limitation that it may only use the data for the purposes that are recognised as legitimate grounds for telecommunications surveillance in § 1(1) and § 3(1) first and second sentence of the Act. Moreover, the statutory framework violates Art. 10 of the Basic Law as it lacks an obligation to label personal data obtained through surveillance. 253

The statutory framework also lacks sufficient safeguards regarding data use by the Federal Government. The protection afforded by Art. 10 of the Basic Law is not limited to acts of the Federal Intelligence Service, as the authority collecting the data, but also applies vis-à-vis the Federal Government as the authority receiving 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. The mandate 254

of the Federal Intelligence Service is limited to observing and analysing situations without executive powers to act on that knowledge; by contrast, the Federal Government is a political organ and the head of the federal executive branch and as such has the means to translate the knowledge obtained into action that could entail significant impairments for persons affected by telecommunications surveillance.

Therefore, data collected for the purposes of providing intelligence reports to the Federal Government may not be used freely by the latter. Rather, the Federal Government may only obtain knowledge of telecommunications contents or circumstances for the purpose of ensuring timely detection of the dangers listed in § 3(1) second sentence nos. 1 to 6 of the Act, so that measures can be taken to avert those dangers. Thus, it is not permissible for the Federal Government to retain or use the data for other purposes. 255

The challenged provision is not *per se* in conflict with the Constitution, as its constitutional shortcomings can be remedied by statutory amendments; therefore, it is not declared void, only incompatible with the Basic Law. It is incumbent upon the legislator to bring the law in conformity with the Constitution. The Basic Law affords the legislator discretion on how to discharge this responsibility. 256

VI.

§ 3(5) first sentence in conjunction with § 3(3) first sentence of the Act obliges the Federal Intelligence Service to share data obtained through telecommunications surveillance with other authorities so that the latter can perform their respective tasks. In this respect, the provision is not fully in line with the requirements deriving from Art. 10 of the Basic Law, nor with Art. 5(1) second sentence of the Basic Law, which must additionally be taken into account. 257

1. Nonetheless, the purpose of the provisions is not objectionable under constitutional law. They aim to ensure that data and information obtained by the Federal Intelligence Service through telecommunications surveillance, in the exercise of its functions, can be used for the purposes of preventing, investigating or prosecuting criminal acts in the event that the data obtained implicates certain individuals in a possible crime. The Basic Law accords great importance to the prevention and investigation of criminal acts. The Federal Constitutional Court has therefore repeatedly emphasised the undeniable need for effective law enforcement and the fight against crime; it has also repeatedly stressed the public interest in establishing the truth in criminal proceedings to the greatest extent possible, so as to convict persons guilty of criminal conduct and exonerate the innocent, and has recognised the effective investigation of crimes, especially serious ones, as a fundamental responsibility of society under the rule of law (cf. BVerfGE 77, 65 <76> with further references; 80, 367 <375>). 258

2. The legislator has also satisfied the requirement that the law specify precisely, for each subject matter, the purposes for which the sharing and further use of personal 259

data is permissible (cf. BVerfGE 65, 1 <46>). […]

3. [The challenged Act does specify such purposes and] the specified purposes are also compatible with the original purpose that justified the collection of the data and the restriction of [the fundamental right to] the privacy of telecommunications resulting from it (cf. BVerfGE 65, 1 <62>). 260

It is true that telecommunications surveillance measures that are not based on any grounds for suspicion may only be carried out by the Federal Intelligence Service for the purposes of strategic surveillance. […] Only this narrow purpose limitation is capable of justifying the breadth and depth of the resulting fundamental rights interferences. If the surveillance measures could, from the outset, be aimed at preventing or prosecuting criminal acts, the relevant statutory powers would be incompatible with Art. 10 of the Basic Law (cf. BVerfGE 67, 157 <180 and 181>). Where fundamental rights set limits to the use of certain methods of data collection, these limits must not be circumvented by allowing data that was lawfully collected for specific purposes to also be used for other purposes that, by themselves, would not have justified the methods used for collecting the data in the first place. 261

Art. 10 of the Basic Law does not generally rule out any form of data sharing with authorities that otherwise are not or should not be permitted to carry out telecommunications surveillance without any grounds for suspicion. However, it must, in any case, be ensured that the receiving authorities do not have access to the entire data records; this is due to the fact that the Federal Intelligence Service, on account of the methods it is permitted to use, necessarily records large quantities of telecommunications that from the outset have no relevance for the receiving authorities. At the same time, it does not contradict the primary purpose for which the data was originally collected if information that is relevant to the prevention, investigation or prosecution of criminal acts – although it was collected for other reasons – is later shared with the authorities specified in § 3(5) of the Act after a careful examination of the obtained data. The challenged provisions governing data sharing satisfy the constitutional requirements applicable in this context: § 3(5) first sentence and § 3(1) first sentence of the Act both specify certain statutory thresholds and § 3(5) second sentence of the Act subjects the sharing to a special review by an official who must be qualified to hold judicial office. 262

4. By contrast, the challenged provisions are not fully compatible with the prohibition of excessive measures. 263

a) The provisions are suitable and necessary for achieving their purpose. 264

[…] 265-266

b) Yet the legislator did not sufficiently satisfy the requirements deriving from the principle of proportionality in its strict sense with regard to statutory provisions that restrict fundamental rights. 267

aa) The principle of proportionality in its strict sense prohibits interferences with fundamental rights that are of such intensity that they are disproportionate to the importance of the matter and the burden imposed on the individual (cf. BVerfGE 65, 1 <54>). To satisfy this principle, restrictions must be appropriate to the importance of the affected fundamental rights. In an overall balancing of the severity of the interference on the one hand, and the weight and urgency of the reasons invoked to justify it on the other hand, the limits of what is reasonable (*zumutbar*) must be observed (cf. BVerfGE 67, 157 <173, 178>; established case-law). 268

[In the present case,] the severity of the interference derives from the fact that the sharing of personal data constitutes an additional encroachment upon telecommunications privacy that could result in even greater impairments than the initial interference. The effects of data sharing are not limited to expanding the group of persons that obtain knowledge of the circumstances and contents of telecommunications. Rather, this knowledge may prompt further measures taken against the persons under surveillance. While the Federal Intelligence Service may not take any measures that directly target individuals, and the political strategies adopted by the Federal Government to counter the danger situations on which the Federal Intelligence Service is required to report are not directed against the respective communicating parties either, the same is not true for the other authorities receiving data shared pursuant to § 3(5) first sentence of the Act. Rather, data sharing will usually prompt the receiving authorities to investigate the persons concerned; this may lead to further inquiries and, in some cases, to the opening of criminal proceedings. 269

With regard to the intensity of the impairment, it is also significant that the Federal Intelligence Service obtained the information through a measure that does not require any grounds for suspicion and that has an indiscriminate effect, and thus affects the privacy of telecommunications in an especially profound manner; it must also be taken into account that the relevant powers of the Federal Intelligence Service are only compatible with Art. 10 of the Basic Law because they merely serve the gathering of strategic intelligence, whereas the communicating parties are identified merely to facilitate the interpretation of the gathered information, which will invariably be fragmented and therefore ambiguous. Under these circumstances, sharing the data with other authorities is only proportionate if it serves overriding interests that outweigh the privacy of telecommunications, and if there is a reliable basis for assuming that the data is relevant to these interests and that the persons concerned are, with sufficient probability, involved in criminal conduct. If this basis is lacking, the limits of what is reasonable have been exceeded. 270

It is therefore imperative that the respective legal interest invoked in this context is of significant weight. It is also imperative that the suspicion that criminal acts are being planned or have been committed be supported by sufficient facts. The greater the weight of the asserted legal interests and the more far-reaching the impairments of these interests that could, or already did, result from the suspected conduct, the more acceptable it becomes to lower the degree of probability required for establishing a 271

violation (or risk thereof) of the respective legal interest, and the degree of certainty required for establishing the facts on which the suspicion is based.

Moreover, the greater the weight attached to the legal interest in question, the more it becomes acceptable to shift the statutory threshold for carrying out data sharing to a purely precautionary stage [before a danger to the legal interest actually arises]. Where the statutory threshold for data sharing merely requires factual indications that certain planning acts that possibly precede criminal conduct are under way, the legal interest must be exceptionally significant (cf. BVerfGE 30, 1 <18>). Accordingly, if the legislator limits the protected legal interests to a few specified high-ranking interests yet the likely damage to these legal interests would be extraordinarily grave, the legislator may set a relatively low threshold for authorising data sharing. If the legislator, by contrast, considerably expands the catalogue of protected legal interests, and the acts it aims to avert include acts that pose a relatively minor threat, it must subject data sharing to a high threshold. 272

bb) The legislator did not in all respects achieve the necessary balance in the design of the statutory prerequisites for data sharing. § 3(5) in conjunction with § 3(3) of the Act is not objectionable to the extent that it permits data sharing regarding persons against whom certain targeted surveillance measures have been lawfully ordered pursuant to § 2 of the Act. However, the constituent elements of the provision are not sufficiently limited in scope with respect to the other statutory grounds for data sharing, namely data sharing based on the suspicion of criminal conduct. This finding follows from an overall assessment of the catalogue of relevant criminal offences, the quality of the factual basis required for establishing the suspicion of criminal conduct, and the temporal scope of what constitutes a threat to the protected legal interests under the statutory regime. 273

The catalogue of criminal offences, based on which the Federal Intelligence Service may share personal data obtained through telecommunications surveillance with other authorities for the purposes of preventing, investigating or prosecuting these crimes, is extraordinarily heterogeneous. It is not limited to felonies but also includes misdemeanours. On the one hand, it includes criminal offences that impair the highest-ranking public interests or even threaten to completely eliminate the ability of the state to protect legal interests. In part, their weight corresponds to, or even exceeds, that of the criminal offences which, pursuant to § 2 of the Act, justify the ordering of targeted surveillance measures against specific individuals. […] On the other hand, however, some offences listed in the catalogue only constitute medium-level crime […]. 274

Moreover, the statutory framework sets relatively lenient standards for the factual basis establishing a suspicion of criminal conduct, especially when compared to the factual basis that is statutorily required for telecommunications surveillance under § 100a of the Code of Criminal Procedure. […] Furthermore, by including planning stages that precede the stage of punishable attempt under § 100a of the Code of 275

Criminal Procedure, the challenged provisions expand the grounds for data sharing to mere preparatory acts [by the person concerned] that fall short of punishable criminal conduct; this renders the challenged provisions more or less devoid of any limitation.

As a consequence, a distinction must be made between the prevention of crime on the one hand, and the investigation and prosecution of crime on the other hand. This follows from the fact that the urgency of data sharing for the purposes of protecting legal interests differs in these situations. The prevention of crime falls in the domain of averting dangers to public security, seeking to protect the affected legal interest from an impending violation and thus prevent harm, whereas by prosecuting criminal offences, the state seeks to punish a violation of protected legal interests that has already occurred, i.e. can no longer be prevented. […] 276

Given that criminal prosecution takes places when a violation of legal interests has already occurred and primarily concerns the question of punishment, it is not justified to lower the statutory threshold for the sharing of personal data obtained through interferences with the privacy of telecommunications pursuant to § 1 and § 3 of the Act to a less strict standard than the one that otherwise applies to law enforcement measures interfering with the privacy of telecommunications pursuant to § 100a of the Code of Criminal Procedure. Given that the interference resulting from data sharing by the Federal Intelligence Service is of comparable severity, it is imperative under constitutional law that the underlying factual basis for the suspicion of a crime be subject to the same standards that apply to measures pursuant to § 100a of the Code of Criminal Procedure. Otherwise, the number of fundamental rights holders affected would exceed the limits of what is reasonable. § 3(3) first sentence of the Act does not satisfy these requirements. […] 277

To the extent that the provision [authorises data sharing] for the prevention of crime, it fails to sufficiently accommodate the protected fundamental rights interests. There is a significant imbalance at the expense of the affected fundamental rights as a result of the following combined factors: any factual indication suffices as the basis of suspicion; mere planning acts [below the threshold of criminal conduct] constitute sufficient grounds; and the statutory grounds include less serious criminal offences. In particular, the combination of accepting any factual indication and including the planning stages of possible crimes [as sufficient grounds] means that these powers authorise purely precautionary action in very early stages before an actual danger to legal interests arises. As a result, the challenged provision not only accepts a lower degree of probability and certainty, but also subjects the exercise of the powers to relatively lenient standards as regards the underlying factual basis. 278

[…] 279

Moreover, the statutory framework is not fully in line with constitutional law with regard to the procedural safeguards for protecting the privacy of telecommunications. […] While the provisions do set out obligations to document the implementation of 280

surveillance measures and the destruction and deletion of data, similar documentation requirements are lacking for the sharing of data. As a result, data sharing cannot be properly reviewed by the competent independent [oversight] bodies or the courts.

It is not possible to interpret the provisions in conformity with the Constitution. […] The legislator must enact new provisions that satisfy the constitutional requirements. 281

VII.

§ 3(7) of the Act is incompatible with Art. 10 of the Basic Law. 282

The provision is not *per se* objectionable under constitutional law. It obliges the receiving authorities to verify that they need the data shared pursuant to § 3(5) of the Act for the purposes specified in § 3(3) of the Act. […] 283

However, just like the provision governing the corresponding powers of the Federal Intelligence Service, § 3(7) of the Act lacks an obligation to label the data; the legislator must impose this obligation on the receiving authorities as a precaution safeguarding the purpose limitation regarding data use. Without such an obligation the data and information stemming from intelligence measures under the Act could, after their relevance to the purposes for which the data was shared has been verified pursuant to § 3(7) of the Act, be stored or merged with other data and information in such a way that it is no longer identifiable as data obtained through strategic telecommunications surveillance. This would circumvent the purpose limitation set out in § 3(3) of the Act. 284

Again, it is not possible to interpret the provision in conformity with the Constitution. It is incumbent upon the legislator to bring the law in conformity with the Constitution. 285

VIII.

§ 3(8) second sentence of the Act, which governs the requirement to notify affected persons of the surveillance measures, is not compatible with the Basic Law. 286

1. It is not objectionable under constitutional law that § 3(8) first sentence of the Act only provides for a limited form of notification of the persons under surveillance. Under Art. 10(2) second sentence in conjunction with Art. 19(4) third sentence of the Basic Law, it is permissible to refrain from notification if the restriction of the privacy of telecommunications serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land*. However, according to the Federal Constitutional Court's established case-law, this only applies on the condition that the person affected be notified *ex post* as soon as it can be ruled out that notification would jeopardise the purpose of the measure or the existence or security of the Federation or of a *Land* (cf. BVerfGE 30, 1 <31 and 32>). […] 287

[…] 288

2. By contrast, § 3(8) second sentence of the Act violates Art. 10 and Art. 19(4) of the Basic Law. 289

Pursuant to this provision, the affected persons need not be notified if their data has been destroyed by the Federal Intelligence Service or a receiving authority within three months. […] 290

[…] 291

The recording of the data in itself already constitutes an interference with the privacy of telecommunications against which legal protection must in principle be afforded. Yet it is the subsequent use of the data that has particularly severe consequences for the affected persons. Therefore, refraining from notification of the persons affected [by the surveillance measures] would be justified only if the collected data was destroyed immediately due to its irrelevance and if no further steps were taken. As § 3(8) second sentence of the Act is not limited to these cases, it restricts Art. 10 and Art. 19(4) of the Basic Law in a disproportionate manner. 292

As the provision can be rendered compatible with fundamental rights by means of statutory amendments, it is not declared void but only incompatible with the Basic Law. It is incumbent upon the legislator to bring the law in conformity with the Constitution. 293

IX.

By contrast, the exclusion of recourse to the courts under § 9(6) of the Act is compatible with the Basic Law. 294

This provision has a constitutional basis in Art. 10(2) second sentence of the Basic Law, which permits the exclusion of recourse to the courts for measures restricting [the privacy of telecommunications] that serve to protect the free democratic basic order or the existence or security of the Federation or of a *Land*, provided that recourse to the courts is replaced by a review carried out by bodies and auxiliary bodies appointed by Parliament. […] 295

[…] 296-297

X.

The provisions on the destruction of data in § 3(6) and in § 3(7) second and third sentence as well as in § 7(4) of the Act are also compatible with the Basic Law. 298

They satisfy the requirement following from Art. 10 of the Basic Law that data obtained through interferences with the privacy of telecommunications be destroyed as soon as it is no longer needed for the purposes justifying the interference. It is not ascertainable that the provisions fall short of the required minimum protection. 299

The provisions are also not objectionable with regard to Art. 19(4) of the Basic Law. The guarantee of effective legal protection does prohibit measures that would essentially frustrate legal protection (cf. BVerfGE 69, 1 <49>). In cases in which it is possible to subject telecommunications surveillance measures carried out by the Federal 300

Intelligence Service to judicial review, the requirement to destroy data that is no longer needed must therefore be reconciled with the guarantee of legal protection in such a way that this guarantee is not circumvented. The provisions are open to such an interpretation.

[…] 301

XI.

§ 9(2) third sentence of the Act, which subjects the surveillance measures to oversight by the Article 10 Committee (*G 10-Kommission*), is incompatible with Art. 10 of the Basic Law. It does not sufficiently guarantee that oversight extends to the entire process of interception and use of the data. Without such an oversight regime, the challenged provisions granting these powers cannot be upheld as constitutional. […] 302

[…] 303

In view of the fact that the Fight Against Crime Act has considerably expanded the Federal Intelligence Service's surveillance activities, it must be ensured that the Article 10 Committee is provided with the staff needed to effectively fulfil its mandate. Moreover, it must be ensured that there is sufficient oversight also at the level of *Land* administrations to the extent that data obtained through interferences with the privacy of telecommunications is shared with *Land* authorities pursuant § 3(5) of the Act. 304

XII.

[…] 305-308

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 - 305-308), http://www.bverfg.de/e/rs19990714_1bvr222694en.html

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