Headnotes

to the Judgment of the First Senate of 19 May 2020

- 1 BvR 2835/17 -

(Federal Intelligence Service – foreign surveillance)

1. **Under Art. 1(3) of the Basic Law, German state authority is bound by fundamental rights; this binding effect is not restricted to German territory.**

   The protection afforded by individual fundamental rights within Germany can differ from that afforded abroad.

   In any event, Art. 10(1) and Art. 5(1) second sentence of the Basic Law, which, in their dimension as rights against state interference, afford protection against telecommunications surveillance, also protect foreigners in other countries.

2. **The current legal framework on the surveillance of foreign telecommunications, on the sharing of intelligence thus obtained with other bodies, and on the cooperation with foreign intelligence services violates the requirement to expressly specify affected fundamental rights, which is enshrined in Art. 19(1) second sentence of the Basic Law. The legislator deliberately considered fundamental rights not to be affected, yet they are applicable in this context, too. The current legal framework also does not satisfy key substantive requirements arising from fundamental rights.**

3. **Art. 10(1) of the Basic Law protects the confidentiality of individual communications as such. Persons asserting a violation of their own fundamental rights are not excluded from the protection afforded by the fundamental rights of the Basic Law merely because they act on behalf of foreign legal entities.**

4. **Legislation on foreign intelligence is covered by the legislative competence for foreign affairs within the meaning of Art. 73(1) no. 1 of the Basic Law. On the basis of this competence, the Federation can confer upon the Federal Intelligence Service not only the task of providing intelligence to the Federal Government with regard to foreign and security policy, but also the separate task of the early detection of dangers with an international dimension that originate from abroad, as long as this does not give rise to operational powers. These dangers must be of such nature and gravity that they can affect the position of the Federal Republic of Germany in the international community and they must be significant to foreign and security policy precisely for this reason.**

5. **In principle, the strategic surveillance of foreign telecommunications is not incompatible with Art. 10(1) of the Basic Law. However, given that it is not based on specific grounds and essentially guided and restricted only by the purpose pursued, the power to conduct strategic surveillance is an exceptional power that must be limited to the gathering of foreign intelligence conducted by an authority that lacks operational powers; it can only be justified by the authority's particular tasks and the specific conditions under which it performs them.**

   Therefore, the legislator must provide for the removal of telecommunications data of Germans and persons within Germany, limits to data that may be collected, the determination of specific surveillance purposes, the structuring of surveillance based on specifically determined measures, special requirements for the targeted surveillance of specific individuals, limits to traffic data retention, a framework governing data analysis, safeguards to protect confidential relationships of trust, the guaranteed protection of the core of private life and obligations to delete data.

6. **Sharing personal data stemming from strategic surveillance is only permissible for the purpose of protecting legal interests of particularly great weight and requires indications of an identifiable danger (*konkretisierte Gefahrenlage*) or sufficiently specific grounds for the suspicion of criminal conduct (*hinreichend konkretisierter Tatverdacht*). Reports provided to the Federal Government are exempt from these requirements insofar as they are exclusively intended to provide political intelligence and prepare government decisions.**

The sharing of personal data requires a formal decision by the Federal Intelligence Service and must be documented specifying the applicable legal basis. Before data is shared with foreign bodies, it must be ascertained that the recipient will handle the data in accordance with the rule of law; if there is any indication that data sharing could jeopardise an individual affected by it, an assessment of possible risks in the specific case is required.

7. **A legal framework on the cooperation with foreign intelligence services only satisfies the constitutional requirements if it ensures that the limits set by the rule of law are not set aside through the mutual sharing of intelligence and that the Federal Intelligence Service essentially remains responsible for the data it has collected and analysed.**

   If the Federal Intelligence Service wants to use search terms determined by a partner intelligence service to automatically share any matches with this service without any detailed content-related analysis, these search terms and the resulting matches must be checked thoroughly. The obligations to obtain assurances that are applicable to the sharing of data with other countries apply accordingly. The sharing of traffic data in its entirety with partner intelligence services requires a qualified need for intelligence relating to specific indications of an identifiable danger. The Federal Intelligence Service must obtain substantial assurances from the partner services regarding their handling of the shared data.

8. **The powers to conduct strategic surveillance measures, to share the intelligence thus obtained and to cooperate with foreign intelligence services are only compatible with the proportionality requirements if they are complemented by independent oversight. Such oversight must be designed as continual legal oversight that allows for comprehensive access to scrutinise the surveillance process.**

   On the one hand, it must be ensured that the key procedural steps of strategic surveillance are subject to independent oversight resembling judicial review by a body that has the power to make final decisions. On the other hand, the measures must be subject to administrative oversight by a body that conducts randomised oversight of the legality of the entire surveillance process on its own initiative.

Institutional independence of the oversight bodies must be guaranteed. This includes that the oversight bodies have a separate budget, independent personnel management, and procedural autonomy. They must be equipped with the personnel and resources required for the effective performance of their tasks. They must have all powers necessary for conducting effective oversight vis-à-vis the Federal Intelligence Service. It must also be ensured that oversight is not obstructed by the third party rule.

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 2835/17 -

Pronounced
on 19 May 2020
Langendörfer
Tarifbeschäftigte
as Registrar
of the Court Registry

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaint

1. of Reporters sans frontières,
   represented by its Directeur général D…,
2. of Ms I…,
3. of Mr G...,
4. of Mr N...,
5. of Mr Z...,
6. of Mr O...,
7. of Mr L...,
8. of Mr M…,

- authorised representatives: 1. Prof. Dr. Matthias Bäcker, LL.M.,
2. Rechtsanwalt Dr. Bijan Moini, -

against § 6(1), (2), (3) and (6),

§ 7(1),

§ 9(4) and (5),

§ 10(3),

§ 13(4),

§ 14(1) first sentence and § 14(2),

§ 15(1),

§ 19(1),

§ 24(1) first sentence, § 24(2) and (3)

of the Federal Intelligence Service Act (*Gesetz über den Bundesnachrichtendienst*) as amended by the Act on the Surveillance of Foreign Telecommunications by the Federal Intelligence Service (*Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes*) of 23 December 2016 (Federal Law Gazette I, *Bundesgesetzblatt* page 3346)

the Federal Constitutional Court – First Senate –

with the participation of Justices

Vice-President Harbarth,

Masing,

Paulus,

Baer,

Britz,

Ott,

Christ,

Radtke

held on the basis of the oral hearing of 14 and 15 January 2020 by

J u d g m e n t:

1. **§§ 6, 7, 13 to 15 of the Federal Intelligence Service Act, as amended by the Act on the Surveillance of Foreign Telecommunications by the Federal Intelligence Service of 23 December 2016 (Federal Law Gazette I, page 3346), and by the Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 of 30 June 2017 (Federal Law Gazette I page 2097), are incompatible with Article 10(1) and Article 5(1) second sentence of the Basic Law (*Grundgesetz*).**

2. **§ 19(1), § 24(1) first sentence, § 24(2) first sentence, § 24(3) of the Federal Intelligence Service Act are incompatible with Article 10(1) and Article 5(1) second sentence of the Basic Law insofar as they authorise the processing of personal data collected in the context of strategic telecommunications surveillance pursuant to §§ 6, 7, 13 to 15 of the Federal Intelligence Service Act.**

3. **The provisions that have been declared incompatible with the Basic Law continue to apply until new provisions have been enacted, at the latest until 31 December 2021.**

4. **The Federal Republic of Germany must reimburse the complainants' necessary expenses incurred in the constitutional complaint proceedings.**

Table of contents

R e a s o n s :

A.

The constitutional complaint challenges the statutory provisions authorising the Federal Intelligence Service (*Bundesnachrichtendienst* – BND) to carry out surveillance of foreign telecommunications, to share the intelligence thus obtained with domestic and foreign bodies and to cooperate with foreign intelligence services in this context. Insofar as they concern cooperation and the surveillance of foreign telecommunications, the challenged provisions were inserted into the Federal Intelligence Service Act (*Gesetz über den Bundesnachrichtendienst* – BNDG) of 20 December 1

1990 (Federal Law Gazette, *Bundesgesetzblatt* – BGBl I p. 2954, 2979), last amended by Art. 4 of the Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 of 30 June 2017 (*Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680*; BGBl I p. 2097), through the Act on the Surveillance of Foreign Telecommunications by the Federal Intelligence Service (*Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes*) of 23 December 2016 (BGBl I p. 3346), which entered into force on 31 December 2016. The law was amended in response to findings and discussions in the First Committee of Inquiry of the 18th German *Bundestag* (*NSA-Untersuchungsausschuss*, Committee of Inquiry into NSA Activities, cf. final report *Bundestag* document, *Bundestagsdrucksache* – BTDrucks 18/12850) and served to clarify the legal framework given that the Federal Intelligence Service had been engaging in these practices prior to the amendment. By contrast, the challenged provisions on data sharing predate the amendment and their wording was not changed by it; however, they now also extend to the sharing of intelligence gathered on the basis of the newly added surveillance powers.

I.

1. […] 2-3

2. Surveillance of foreign telecommunications is solely aimed at intercepting telecommunications of foreigners in other countries. It is part of the Federal Intelligence Service's general task of conducting surveillance, which, according to § 1(2) first sentence BNDG, comprises the gathering and analysis of the information necessary to obtain intelligence on other countries that is significant to the foreign and security policy of the Federal Republic of Germany. 4

The Federal Intelligence Service uses different sources of information to fulfil this task. These can be divided into four pillars: gathering and analysing generally accessible information, analysing images – primarily satellite images –, gathering and analysing information obtained through human intelligence, and signals intelligence (SIGINT) collected by the department for technical surveillance. Strategic surveillance of foreign telecommunications, which is at issue in the present proceedings, is part of signals intelligence. […] 5

The challenged provisions govern strategic telecommunications surveillance. This form of surveillance is characterised by the use of telecommunications transmission channels or networks and applies filtering mechanisms to separate data relevant for intelligence work from the entire telecommunications data transmitted via the networks. By definition, it thus indiscriminately affects a large number of persons and is usually not tied to specific grounds or suspicions. Instead, it is a purely precautionary measure that primarily serves to obtain indications, suspicions, general intelligence and situation reports in relation to matters that the Mission Statement of the Federal Government (*Auftragsprofil der Bundesregierung*; […]) considers significant for the 6

Federal Republic of Germany's actions in foreign and security policy matters. In addition, strategic telecommunications surveillance also allows for and is aimed at the gathering of intelligence relating to specific individuals.

Besides the powers to carry out strategic telecommunications surveillance of foreigners in other countries, which are challenged in these proceedings, the Federal Intelligence Service has the powers to carry out strategic surveillance of international telecommunications traffic, i.e. telecommunications between foreigners in other countries on one side and persons within Germany or German citizens on the other. This is in addition to its powers to carry out measures restricting [the fundamental right under Article 10 of the Basic Law] in the individual case. Those powers, which are not at issue here, are set out in the Article 10 Act (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, *G 10-Gesetz*) of 26 June 2001 (BGBl I p. 1254, 2298), last amended by Article 12 of the Act of 17 August 2017 (BGBl I p. 3202) and are designed differently. Other authorities, in particular the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*) – Germany's domestic intelligence service –, do not have such powers. 7

3. The challenged provisions set out specific rules for collecting data from within Germany and processing it (§ 6 BNDG), and for further processing data collected from abroad (§ 7(1) BNDG). […] 8

[…] 9

They provide a basis for collecting any information and data from those networks that are determined by the Federal Chancellery (*Bundeskanzleramt*) in a warrant ('bulk interception warrant' – *Netzanordnung*, cf. § 6(1) second sentence, § 9(1), (3) and (4) BNDG). […] 10

[…] 11

4. §§ 13 to 15 BNDG set out rules for the cooperation between the Federal Intelligence Service and foreign intelligence services, including the automated sharing of data with foreign authorities. […] 12

5. Besides these special rules for collecting, processing, storing, deleting and sharing data obtained through the surveillance of foreign telecommunications, the general provisions of the Federal Intelligence Service Act on using, processing, storing, rectifying, deleting and sharing personal data held by the Federal Intelligence Service apply (§§ 19, 20 and 24 BNDG); these provisions were not modified by the amendment of 23 December 2016. According to these general provisions, the Federal Intelligence Service may store, alter and use personal data obtained through the surveillance of foreign telecommunications insofar as this is necessary for performing its tasks (§ 19(1) BNDG). It must rectify and delete data that is incorrect or no longer necessary for the performance of its tasks; in this respect, inspection periods of up to ten years are permissible (§ 20(1) BNDG, § 12 of the Federal Protection of the Constitution Act, *Bundesverfassungsschutzgesetz* – BVerfSchG). § 24 BNDG and the provisions of 13

the Federal Protection of the Constitution Act referred to therein authorise the Federal Intelligence Service to share, in the individual case, the information obtained by it, especially personal data, with domestic and foreign bodies specified in the provisions.

6. Further details regarding data collection and processing, regarding monitoring responsibilities within the Federal Intelligence Service and regarding data sharing in the context of cooperation must be set out in intelligence service manuals that require the approval of the Federal Chancellery (§ 6(7), § 15(3) fifth sentence BNDG). Beyond these legal requirements, the technical and practical details of the entire process of data collection and analysis, cooperation and data sharing are set out in intelligence service manuals that are not publicly accessible. […] 14

7. Even before the challenged powers were enacted, and in the exercise of these powers ever since the enactment, a practice of conducting strategic surveillance of foreign telecommunications has evolved that consists of different steps. 15

a) First, the Federal Intelligence Service gains access to telecommunications data by intercepting signals from telecommunications networks either by using its own equipment or by having telecommunications service providers divert data flows pursuant to § 8 BNDG. […] 16

[…] 17-18

b) The data that becomes accessible through the diversion of data or through other interception methods is transmitted to the Federal Intelligence Service's interception systems, initiating a multi-step and fully automated process of sorting and analysis, at the end of which temporarily saved data is stored or deleted. The data undergoes technical processing to categorise it into different types of data (for example data from streaming, browsing history data, telecommunications data) and to remove data that is found to be irrelevant for technical reasons. Following this, the telecommunications data is electronically filtered to identify and remove data that is not part of the surveillance of foreign telecommunications due to the involvement of German citizens and persons within Germany (so-called DAFIS filtering mechanism). Different formal parameters relating to communications data (e.g. use of a German top-level domain) are used to assess whether the intercepted telecommunications processes are connected to German citizens or persons within Germany; in addition, the data is compared with a list, maintained by the Federal Intelligence Service, of telecommunications identifiers that can be attributed to Germans or persons within Germany ("Article 10 List"). It is in dispute between the parties how reliable this filtering system is and whether better filtering mechanisms are technically possible. According to the Federal Government, the current system can match IP addresses to a specific state with 98% certainty. Additionally, the Federal Intelligence Service uses further formal parameters and communications data in its filtering process in order to also identify data that is connected to persons within Germany or German citizens but is exclusively matched to foreign IP addresses, for example due to intermediary servers located abroad or due to the use of hotspots. It is unknown how many telecommunications 19

processes are falsely categorised as purely foreign telecommunications.

[…] 20

c) The Federal Intelligence Service collects and stores all traffic data that is left after the DAFIS filtering mechanism was applied (§ 6(6) first sentence BNDG) without using any selectors, and later performs primarily computer-based analysis through cross-checking and other methods. 21

d) However, pursuant to § 6(2) BNDG, content data is only stored and analysed beyond temporary storage required for technical reasons if elements of a telecommunications process are identified as relevant during the computer-based cross-checking against predetermined search terms (selectors). According to the submissions made by the Federal Government and the requirements laid down in the relevant intelligence service manual (DV SIGINT), before they are actively used (“steering”), the search terms are checked by a department within the Federal Intelligence Service (“Quality Assurance SIGINT”) as to their conformity with the Service’s mandate, their legal permissibility – in particular with regard to proportionality – and their plausibility. Content data collected by the Federal Intelligence Service’s systems that has not been selected on the basis of search terms is deleted in its entirety from the systems once it has been cross-checked. 22

The selectors are divided into content-related and formal search terms, yet the Federal Intelligence Service primarily uses the latter (according to the Federal Government, they make up approximately 90% of selectors). These formal search terms are communication parameters, such as telecommunications identifiers or email addresses that can be attributed to persons, entities, groups or phenomena the Federal Intelligence Service considers relevant. The Federal Intelligence Service can use such search terms to identify all telecommunications that are sent to the identifier or address that is used as a search term, are sent from it or contain it and separate these telecommunications from the rest of the intercepted data for storage. According to the Federal Government, approximately 5% of search terms serve to obtain targeted information on individuals in view of measures to be taken against them; in all other cases, the persons behind the steered search terms are only sometimes known, and they themselves and their conduct are not the focus of intelligence gathering. 23

[…] 24

e) Following the selection and storage of content data by means of search terms, the data is subject to further analysis. This step primarily involves manually screening data as to its relevance for the Federal Intelligence Service. Currently, an average of 260 data transmissions are identified and forwarded to the relevant departments every day. According to the Federal Government, it is in this context that the protection of the core of private life required by § 11 BNDG is implemented in practice – along with an assessment of the relevance of the data and manual screening to check whether international or domestic telecommunications were intercepted inad- 25

vertently. The Federal Government submits that the requirements regarding the protection of the core of private life do not have any practical effect on the previous steps. According to the relevant intelligence service manual (DV SIGINT) and submissions of the Federal Government, protected communications of persons entitled to refuse to give evidence under § 53 of the Code of Criminal Procedure (*Strafprozessordnung* – StPO) are taken into account during manual screening; such communications may only be used if their particularly significant informative value is balanced against conflicting confidentiality interests and outweighs them.

f) §§ 13 to 15 BNDG enshrine the practice of cooperation between intelligence services into law for the first time. Such cooperation was a major focus of the investigations conducted by the NSA Committee of Inquiry (cf. BTDrucks 18/12850, pp. 516 *et seq*.; 706 *et seq*.; 761 to 1007). According to the legislative documents (BTDrucks 18/9041, p. 29) and submissions of the Federal Government, such cooperation aims to facilitate the effective use of intelligence resources, to expand the resources from which intelligence services can gather data and to continually share intelligence know-how, particularly technical abilities and suitable search terms. 26

[…] 27-29

8. These processes are subject to both specific and general rules on transparency, internal monitoring and oversight. Internally, the Federal Intelligence Service is obliged to label collected data (§ 10(1) BNDG); special documentation is required for cases of impermissible data processing (§ 10(6) and § 11 fourth sentence BNDG) and for automatic data sharing with foreign partners (§ 15(2) BNDG). Affected persons have rights to information, yet the exercise of such rights does not extend to the origin of the data and requires that affected persons demonstrate a special interest in the requested information (§ 22 BNDG). Notification requirements only apply in cases where telecommunications in which Germans or persons within Germany are involved are collected impermissibly and subsequently stored (§ 10(4) second sentence BNDG); there are no notification requirements vis-à-vis affected foreigners in other countries, even in case data is collected or processed impermissibly. 30

§ 16 BNDG establishes a special oversight body, the Independent Body (*Unabhängiges Gremium*); its specific oversight powers derive from §§ 6 to 15 BNDG. General oversight to ensure data protection falls to the Federal Commissioner for Data Protection and Freedom of Information (§§ 32 and 32a BNDG). A department within the office of the Federal Commissioner for Data Protection and Freedom of Information is competent to oversee the Federal Intelligence Service. In addition, special oversight competences are assigned to the Article 10 Commission (*G 10-Kommission*) in cases where notification is deferred pursuant to § 10(4) BNDG. The power to conduct general parliamentary oversight falls to the Parliamentary Oversight Body (*Parlamentarisches Kontrollgremium*) and its Permanent Representative, and this body also has specific powers in relation to the surveillance of foreign telecommunications (§ 6(7) third sentence, § 13(5) second sentence BNDG). 31

According to the former chair of the Independent Body and the Federal Commissioner for Data Protection, oversight by either body is restricted in practice by the need of partner intelligence services to maintain secrecy and by existing confidentiality agreements (third party rule). 32

II.

With their constitutional complaint, the complainants assert that their fundamental right to the privacy of telecommunications under Art. 10 of the Basic Law (*Grundgesetz* – GG) has been violated. Insofar as they work as journalists, they also claim that their fundamental right to freedom of the press under Art. 5(1) second sentence GG has been violated, given that the Federal Intelligence Service Act does not contain special rules for the protection of confidentiality between the press and their sources in the context of strategic surveillance of foreign telecommunications. Finally, complainant no. 1 and complainants nos. 3 to 5 also assert a violation of the general guarantee of the right to equality under Art. 3(1) GG because, as a legal entity based in an EU Member State and as EU citizens, they do not enjoy the same protection as German citizens. 33

1. All complainants submit that they are affected by the authorisations granted to the Federal Intelligence Service and its actions based thereon in the context of surveillance of foreign telecommunications. […] 34

[…] 35

2. […] 36-37

3. […] 38

4. […] 39

5. […] 40-41

III.

In the constitutional complaint proceedings, statements were submitted by the Federal Government, the Bavarian *Land* Government, the respective Federal Commissioners for Data Protection and Freedom of Information and the Sixth Senate deciding on appeals on points of law (*Revisionssenat*) of the Federal Administrative Court (*Bundesverwaltungsgericht*). 42

[…] 43-53

IV.

Prior to the oral hearing, the Federal Government, the Federal Commissioner for Data Protection and Freedom of Information, the eco Association of the German Internet Industry e.V. (*eco-Verband der deutschen Internetwirtschaft e.V.*), T-Systems International GmbH and the Chaos Computer Club e.V. submitted written statements in response to a list of questions provided by the Federal Constitutional Court regard- 54

ing the technical aspects of international telecommunications networks and the possibilities and dimensions of intelligence work carried out by the Federal Intelligence Service.

In the oral hearing, the Court heard the complainants, the Federal Government, the Federal Intelligence Service, the Parliamentary Oversight Body, the Article 10 Commission and the Federal Commissioner for Data Protection and Freedom of Information. As experts, the Court also heard the Federal Government's former IT security officer Martin Schallbruch as well as Barrister Dr Tom Hickman QC, Standing Counsel to the Investigatory Powers Commissioner's Office of the United Kingdom. As expert third parties, the Court heard the Judge at the Federal Court of Justice (*Bundesgerichtshof*) Gabriele Cirener as the former chair of the Independent Body, the eco Association of the German Internet Industry e.V., T-Systems International GmbH and the Chaos Computer Club e.V. 55

B.

The constitutional complaint is admissible. 56

I.

The complainants lodged a constitutional complaint against statutes (*Rechtssatzverfassungsbeschwerde*) challenging powers to carry out surveillance and to share data which are conferred upon the Federal Intelligence Service for the surveillance of foreign telecommunications. The complainants directly challenge the respective provisions conferring the powers in question upon the Federal Intelligence Service, but they also indirectly challenge further provisions which provide a framework to ensure the proportionality of these powers and without which their constitutionality cannot be assessed. Based on a reasonable interpretation, the constitutional complaint thus directly challenges §§ 6, 7 and §§ 13 to 15 BNDG, but to assess these provisions, §§ 9 to 11 and §§ 16, 20, 22, 32, 32a BNDG must also be incorporated into the review. As the latter provisions give specific shape to the challenged powers, the Court's review must include them and determine whether they are applicable and tenable under constitutional law. In addition, the complainants challenge § 19(1) and § 24 BNDG as well as further provisions referred to therein to the extent that they are applicable to the handling of data obtained through strategic surveillance pursuant to §§ 6, 7 and 13 to 15 BNDG. 57

II.

The complainants have standing. 58

1. The complainants assert a violation of their fundamental rights under Art. 10(1), Art. 5(1) second sentence and Art. 3(1) GG. […] 59

[…] 60

2. Complainants nos. 1 to 7 do not lack standing on the grounds that they are a for- 61

eign legal entity or foreigners living abroad who are invoking the fundamental rights of the Basic Law. As of yet there has been no definitive answer to the question if and to what extent citizens of other states can invoke the fundamental rights of the Basic Law to challenge measures of the German state in other countries. In its decision of 14 July 1999, the Federal Constitutional Court neither made a positive determination in this regard, nor did it rule this out (cf. Decisions of the Federal Constitutional Court, *Entscheidungen des Bundesverfassungsgerichts* – BVerfGE 100, 313 <362 *et seq*.>). Thus, a violation of fundamental rights appears at least possible.

3. Complainant no. 1 also does not lack standing on the grounds that it is a legal entity based abroad. The complainant sufficiently demonstrates that the extension of fundamental rights protection to legal entities based in the European Union may apply to it (see a) below). By reason of their nature, the fundamental rights invoked by the complainant meet the requirements regarding the applicability of Art. 19(3) GG (see b) below). 62

a) Based on the European Treaties, the Federal Constitutional Court's case-law recognises that fundamental rights protection may be extended to legal entities based in the European Union. Legal entities based in other EU countries are afforded the same treatment as domestic legal entities as regards fundamental rights if the affected EU legal entity operates within the scope of application of EU law and if it has a sufficient link to domestic matters that makes it appear necessary that the fundamental rights apply to it in the same way as they apply to domestic legal entities (cf. BVerfGE 129, 78 <94 *et seq*.>). 63

Based on the foregoing, an extension of fundamental rights protection to the complainant as a foreign legal entity must at least be considered. In the present case, a link to domestic matters that gives rise to a need for protection on the part of complainant no. 1 can be inferred from the fact that the challenged provisions provide a basis for carrying out surveillance from within Germany and also give effect to an interest of German authorities in obtaining information about activities undertaken abroad by persons under surveillance; thus, the complainant becomes a specific target of surveillance. 64

Moreover, the complainant's activities potentially fall within the scope of application of EU law as is required for an extension of fundamental rights protection to the complainant. This possibility must be considered, for instance, because the complainant makes use of the fundamental freedoms guaranteed to it under primary law when it accepts cross-border services, thus exercising its passive freedom to provide services enshrined in Art. 56 TFEU. However, under Art. 4(2) third sentence TEU, national security in particular remains the sole responsibility of the individual Member State, which could result in certain activities not falling within the scope of EU law, at least with regard to some of the tasks of the Federal Intelligence Service. If and to what extent that is the case has not yet been determined under EU law either (cf. Reference for a preliminary ruling from the Investigatory Powers Tribunal London 65

[United Kingdom] made on 31 October 2017, Privacy International, C-623/17, OJ EU 2018/C 022/41; Reference for a preliminary ruling from the Conseil d'État [France] made on 3 August 2018, La Quadrature du Net and Others, C-511/18, OJ EU 2018/C 392/10 and French Data Network and Others, C-512/18, OJ EU 2018/C 392/11 regarding Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector – Directive on privacy and electronic communications, OJ EU 2002/L 201/37, hereinafter: Directive 2002/58/EC).

When determining whether the constitutional complaint is admissible, there is no need to decide if or to what extent this matter falls within the scope of application of EU law. This is because, in any case, complainant no. 1 demonstrated that a right might have been violated in respect of which they can lodge a constitutional complaint (cf. BVerfGE 125, 39 <73>; 129, 78 <91>). It is not necessary to request a preliminary ruling from the Court of Justice of the European Union pursuant to Art. 267(3) TFEU given that the constitutional complaint is admissible in any case and that the question is not decisive for determining whether the constitutional complaint is well-founded (see para. 328 below). 66

b) By their nature, the asserted fundamental rights, Art. 10(1) GG, Art. 5(1) second sentence GG and Art. 3(1) GG, are applicable to legal entities as provided for by Art. 19(3) GG (cf. regarding Art. 10(1) GG: BVerfGE 100, 313 <356>; 106, 28 <43>; regarding Art. 5(1) second sentence GG: BVerfGE 80, 124 <131>; 95, 28 <34>; 113, 63 <75>; regarding Art. 3(1) GG: BVerfGE 21, 362 <369>; 42, 374 <383>; 53, 336 <345>). 67

4. Complainants nos. 6 and 8 do not lack standing on the grounds that they act on behalf of foreign legal entities (*Funktionsträger*), which, pursuant to Art. 19(3) GG, are not themselves holders of fundamental rights. 68

[…] It is true that persons acting on behalf of legal entities can only invoke their own fundamental rights; they cannot invoke fundamental rights of the legal entities on whose behalf they act. However, insofar as their own fundamental rights are affected, they cannot be deprived of protection merely because they act on behalf of a foreign legal entity that cannot invoke the fundamental rights of the Basic Law under Art. 19(3) GG ([…]). […] 69

[…] 70

III.

The challenged provisions affect the complainants directly, individually and presently. Their constitutional complaint thus satisfies the requirements for constitutional complaints lodged directly against a statute. 71

1. The complainants are directly affected. It is true that the challenged powers require further implementation measures. However, it must also be assumed that per- 72

sons are directly affected by a law requiring implementation in cases where seeking legal recourse is not possible because they have no way of knowing whether the implementation measure was carried out, or where *ex post* disclosure is provided for, but can be refrained from, even in the long term, based on broad exceptional grounds (BVerfGE 150, 309 <324 para. 35> with further references; established case-law). […]

2. The challenged provisions also affect the complainants individually and presently. 73

[…] 74-76

IV.

The constitutional complaint satisfies the requirements arising from the principle of subsidiarity. 77

1. Under the principle of subsidiarity, complainants are, in principle, obliged to use any means at their disposal that might remedy the asserted violation of fundamental rights; this also applies to lodging a constitutional complaint against statutes. Legal remedies that are appropriate (*zumutbar*) in this context may also include a declaratory action or injunctive relief, which allow for review of decisive factual or legal questions of ordinary law by ordinary courts (for a general overview see, most recently, BVerfGE 150, 309 <326 *et seq*. para. 41 *et seq*.> with further references). However, the situation is different where only limits to the interpretation of statutes are concerned that directly follow from the Constitution. A prior decision by ordinary courts is not required insofar as the assessment of a statute only raises questions of a constitutional nature that must be answered by the Federal Constitutional Court and when a prior review by the ordinary courts will probably not provide a better basis for its decision (cf. BVerfGE 123, 148 <172 and 173>; 143, 246 <322 para. 211>; established case-law). In this respect, it remains true that constitutional complaints lodged directly against a statute are mostly admissible even without prior recourse to the ordinary courts (cf. BVerfGE 150, 309 <326 and 327 para. 44>). 78

2. Based on these considerations, the complainants were not required to first have recourse to the ordinary courts. […] 79

Furthermore, due to the current case-law of the administrative courts, legal protection in this matter could not be achieved in practice. The Federal Administrative Court has previously declared inadmissible actions regarding strategic telecommunications surveillance on the grounds that the plaintiffs could not point to sufficiently specific measures carried out by the Federal Intelligence Service (cf. Decisions of the Federal Administrative Court, *Entscheidungen des Bundesverwaltungsgerichts* – BVerwGE 157, 8 <12 and 13 para. 16 *et seq*.>; 161, 76 <78 para. 14>); it cannot be ascertained that the complainants in the case at hand could have satisfied those requirements. 80

V.

The constitutional complaint was also lodged within the time limit set out in § 93(3) of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz* – BVerfGG). 81

[…] 82-83

VI.

Since the surveillance of foreign telecommunications does not concern the implementation of binding EU law, the assessment of whether the challenged provisions are valid under constitutional law must be based on the fundamental rights of the Basic Law. Thus, the Federal Constitutional Court is competent to decide and the constitutional complaint is admissible in this respect. This applies irrespective of whether EU fundamental rights may also be applicable (cf. BVerfG, Order of the First Senate of 6 November 2019 - 1 BvR 16/13 -, para. 39 – Right to be forgotten I). 84

This does not have any bearing on the question whether further legal requirements directly follow from secondary EU law, in particular from Art. 15(1) of Directive 2002/58/EC with regard to the extent of the obligations imposed on telecommunications providers. It is not for the Federal Constitutional Court to interpret and apply ordinary EU legislation; this task is incumbent upon the ordinary courts in cooperation with the Court of Justice of the European Union (cf. BVerfGE 148, 40 <48 and 49 para. 22>). 85

C.

The constitutional complaint is well-founded. The challenged provisions must be measured against the fundamental rights of the Basic Law; they amount to interferences with Art. 10(1) and Art. 5(1) second sentence GG (see I. to III. below). The interferences are not justified because the challenged provisions are formally unconstitutional (see D. below). They also do not satisfy the key substantive requirements arising from Art. 10(1) and Art. 5(1) second sentence GG (see E. below). 86

I.

The fundamental rights of the Basic Law are binding upon the Federal Intelligence Service and the legislator that sets out its powers, irrespective of whether the Federal Intelligence Service is operating within Germany or abroad. The protection afforded by Art. 10(1) and Art. 5(1) second sentence GG also applies to telecommunications surveillance of foreigners in other countries. 87

1. Art. 1(3) GG provides that German state authority is comprehensively bound by the fundamental rights of the Basic Law. No restrictive requirements that make the binding effect of fundamental rights dependent on a territorial connection with Germany or on the exercise of specific sovereign powers can be inferred from the provision. In any event, this holds true for the fundamental rights at issue in the present case, which, in their dimension as rights against state interference, afford protection 88

against surveillance measures.

a) According to Art. 1(3) GG, the fundamental rights of the Basic Law bind the legislature, the executive and the judiciary as directly applicable law. The provision does not contain an explicit restriction to German territory. There was also no unspoken consensus at the time the Basic Law came into existence from which an exemption could be derived according to which fundamental rights were not applicable to the actions of German state organs abroad ([…]). Rather, particularly in response to the Nazi reign of violence and tyranny, Art. 1(3) GG aimed to achieve a comprehensive binding effect of fundamental rights rooted in human dignity; as early as 1949, the provision was embedded in the conviction that the Federal Republic of Germany had to find its place in the international community as a partner that abides by the rule of law ([…]). This is reflected in the Basic Law's preamble and in particular in Art. 1(2) GG and Arts. 24 and 25 GG. Even though the question whether fundamental rights would be binding outside of German territory was not addressed during the deliberations preceding the adoption of the Basic Law and even though the type of surveillance measures targeting other countries that are possible today were unimaginable at the time, it cannot be inferred from the Basic Law's legislative history that fundamental rights protection was always meant to end at the national border. Rather, the Basic Law's aim to provide comprehensive fundamental rights protection and to place the individual at its centre suggests that fundamental rights ought to provide protection whenever the German state acts and might thereby create a need for protection – irrespective of where and towards whom it does so. 89

b) Under Art. 1(3) GG, fundamental rights as rights of the individual against state interference are not only binding in constellations in which the German state acts vis-à-vis the affected persons as a sovereign power that has the monopoly on the use of force ([…]). Above all, such a restriction, which would largely rule out the binding effect of fundamental rights in the context of foreign surveillance, cannot be inferred from the fact that Art. 1(3) GG does not refer to German state authority as such, but names the different state functions legislature, executive and judiciary. This does not restrict the instances in which fundamental rights are binding, but rather makes it clear that fundamental rights provide protection vis-à-vis all state authority known to the traditional doctrine of the separation of powers – they also provide protection vis-à-vis the legislature in particular, which was not self-evident at the time ([…]). […] 90

State authority is bound comprehensively and universally by the fundamental rights, irrespective of the specific functions, the types of action or the respective object of the exercise of state functions ([…]).State authority must be understood broadly, covering not only orders and prohibitions or measures based on sovereign powers. Fundamental rights are binding in relation to any decision that can claim to be made on behalf of all citizens at the relevant level of decision-making within the state. This includes both sovereign and non-sovereign measures, statements and actions. Thus, any action of state organs or organisations constitutes an exercise of state authority that is bound by fundamental rights within the meaning of Art. 1(3) GG because such 91

actions are performed in the exercise of their mandate to serve the common good (BVerfGE 128, 226 <244>). The binding effect of fundamental rights and the political responsibility for decisions are inextricably linked (cf. BVerfG, Order of the First Senate of 6 November 2019 - 1 BvR 16/13 -, para. 42 – Right to be forgotten I).

c) The binding effect of fundamental rights on the German state, even when it acts abroad, is not limited to a mere objective legal duty ([…]). Rather, it corresponds with a legal right afforded anyone recognised as a protected fundamental rights holder by the fundamental right in question. The Basic Law does not provide for fundamental rights that bind the state vis-à-vis individual fundamental rights holders without also providing the individual with a corresponding subjective right. It is a key part of fundamental rights protection under the Basic Law that fundamental rights are rights of the individual. 92

2. German state authority is bound by fundamental rights even in relation to actions taken vis-à-vis foreigners in other countries; this is also in line with Germany's participation in the international community. 93

a) In Art. 1(2) GG, the Basic Law acknowledges inviolable and inalienable human rights as the basis of every community, of peace, and of justice in the world. The Basic Law thus places fundamental rights in the context of international human rights guarantees that seek to provide protection beyond national borders and are afforded to individuals as human beings. Accordingly, Art. 1(2) and Art. 1(3) GG build upon the guarantee of human dignity enshrined in Art. 1(1) GG. Given this essentially universal nature of fundamental rights protection, in the codification of fundamental rights the Basic Law deliberately differentiates between human rights and rights afforded only German citizens. However, this does not mean that human rights should also be limited to domestic matters or state action in Germany. There is nothing in the wording of the Basic Law to suggest such an understanding. In particular, such a restriction cannot be inferred from the preamble of the Basic Law; its reference to the "German people in the *Länder*" is not a reference to German territory, but is worded from the perspective of the constitutional legislator and emphasises the responsibility of the German people in a united Europe and in the world ([…]). 94

Furthermore, the terminological distinction between "inviolable and inalienable human rights" in Art. 1(2) GG and the "following fundamental rights" in Art. 1(3) GG can also not be used as an argument against the integration of fundamental rights into the context of universal human rights. In this respect, too, nothing in the Basic Law's wording and systematic concept suggests that this differentiation ought to be interpreted as relating to territory or as indicating separate territorial scopes of application. On the contrary, the fundamental rights of the Basic Law (Art. 1(3) GG) are all linked to the guarantee of human rights; this is also shown by the Federal Constitutional Court's established case-law, according to which the fundamental rights of the Basic Law must be interpreted in light of international human rights guarantees (cf. BVerfGE 111, 307 <317 and 318>; 128, 282 <306 and 307>; 128, 326 <367 and 368>; 95

142, 313 <345 para. 88>; 148, 296 <351 para. 128>; BVerfG, Order of the First Senate of 6 November 2019 - 1 BvR 16/13 -, para. 58 – Right to be forgotten I). Moreover, the principles enshrined in Art. 1(2) GG constitute an absolute limit, within the meaning of Art. 79(3) GG, for restrictions of fundamental rights protection by the Constitution-amending legislator (cf. BVerfGE 84, 90 <120 and 121>; 141, 1 <15 para. 34>).

This link between fundamental rights and human rights guarantees is incompatible with the notion that the applicability of the fundamental rights of the Basic Law ends at the national border, which would exempt German authoritiesfrom having to adhere to fundamental rights and human rights when they act abroad vis-à-vis foreigners. Such a notion would run counter to the Basic Law's aim of ensuring that every person is afforded inalienable rights on the basis of international conventions and beyond national borders – including protection from surveillance (cf. Art. 12 of the Universal Declaration of Human Rights, Art. 17(1) of the International Covenant on Civil and Political Rights). Given the realities of internationalised political action and the ever increasing involvement of states beyond their own borders, this would result in a situation where the fundamental rights protection of the Basic Law could not keep up with the expanding scope of action of German state authority and where it might – on the contrary – even be undermined through the interaction of different states. Yet the fact that the state as the politically legitimated and accountable actor is bound by fundamental rights ensures that fundamental rights protection keeps up with an international extension of state activities. 96

b) The European Convention on Human Rights, which constitutes a guideline for the interpretation of fundamental rights, also suggests such an understanding of the scope of the fundamental rights of the Basic Law (cf. BVerfG, Order of the First Senate of 6 November 2019 - 1 BvR 16/13 -, para. 58 with further references – Right to be forgotten I). It has not yet been comprehensively determined to what extent its guarantees apply to actions of the Contracting Parties outside of their own territory. The European Court of Human Rights is mainly guided by the criterion of whether a state exercises effective control over an area outside its own territory; on this basis, it has in many cases affirmed the applicability of Convention rights abroad (cf. in summary ECtHR [GC], Al-Skeini and Others v. the United Kingdom, Judgment of 7 July 2011, no. 55721/07, §§ 132 *et seq*. with further references; cf. also Aust, Archiv des Völkerrechts 52 <2014>, p. 375 <394 *et seq.*> with further references). However, there has been no final determination as to whether protection is afforded against surveillance measures carried out by Contracting Parties in other states. 97

In a decision that has not become final yet, the First Section of the European Court of Human Rights measured the implementation of surveillance measures targeting persons abroad against the standards of the Convention without any restrictions and found such measures to be in violation of the Convention. The complainants in this case included foreign nationals who were not present or resident in the state against which the applications were directed (cf. ECtHR, Big Brother Watch and Others v. the United Kingdom, Judgment of 13 September 2018, no. 58170/13 and others, § 271). 98

Similarly, a Swedish foundation challenged strategic foreign surveillance powers under Swedish law that exclude domestic communications. The European Court of Human Rights reviewed these powers without calling into question the Convention's applicability abroad (cf. ECtHR, Centrum för Rättvisa v. Sweden, Judgment of 19 June 2018, no. 35252/08). Both proceedings are now pending before the Grand Chamber.

Irrespective of the outcome of these proceedings, the European Convention on Human Rights does not stand in the way of the applicability of German fundamental rights abroad. This is because the Convention is an international treaty with its own separate scope of application; no direct inferences can be drawn from it with regard to the scope of fundamental rights protection under the Basic Law. In any case, the Convention does not rule out further-reaching fundamental rights protection by the Contracting Parties (Art. 53 ECHR). 99

c) In the case at hand, it is also not necessary to seek a delimitation from and coordination with other states and legal systems, which is the only possible reason that could stand in the way of the applicability of fundamental rights to German state authority abroad; this issue was discussed, and left unresolved, by the Federal Constitutional Court with regard to excluding the applicability of Art. 10 GG in relation to foreign matters (cf. BVerfGE 100, 313 <362 *et seq*.>). 100

The binding effect of German fundamental rights entails accountability and responsibility solely on the part of German state organs. It only applies to autonomous political decisions made by the Federal Republic of Germany and solely limits Germany's own latitude. Accordingly, in other countries German fundamental rights – in their dimension as rights against state interference – are only applicable vis-à-vis German state authority and are thus in line with the restrictions arising from the principle of non-intervention under international law. Thus, the binding effect of fundamental rights does not amount to a violation of the principle of non-intervention or to a restriction of other states' executive or legislative powers. It neither imposes German law on other states, nor does it supplant the fundamental rights of other states. In particular, the binding effect of fundamental rights does not extend German state powers abroad, but limits potential courses of action of German state authority. 101

Thus, the applicability of fundamental rights (in this case Art. 10(1) GG) has no effect on the legal order of other states; authorisations to carry out surveillance measures that are tied to the applicability of fundamental rights are also not binding within the legal systems of other states. It merely follows from the applicability of fundamental rights and the requirement of a statutory provision that a statutory basis must be created for surveillance measures carried out by German bodies in relation to foreigners in other countries. This does not predetermine whether and to what extent such powers are actually created and used. Nor does this say anything about the justification of individual measures based on such powers with regard to their effects vis-à-vis the targeted state. 102

In light of the foregoing, the binding effect of fundamental rights as such does not 103

answer the question whether such measures are permissible under international law. Other states are of course free to defend themselves against such measures – just as Germany may, under domestic constitutional law, defend itself against surveillance measures of foreign intelligence services in Germany (see para. 249 below). Therefore, the binding effect of fundamental rights on German state authority does not place a burden on other states that could give rise to concerns under international law ([…]). Internationally, it is quite common to create statutory bases for surveillance measures targeting foreigners in other countries. Such statutes give rise to merely domestic authorisations (cf. Gusy, in: Schenke/Graulich/Ruthig [eds.], Sicherheitsrecht des Bundes, 2nd ed. 2019, § 1 BNDG para. 56; e.g. in respect of the United States: Section 702 Foreign Intelligence Surveillance Act; cf. Renan, in: Goldman/Rascoff [eds.], Global Intelligence Oversight, 2016, p. 121 <123 *et seq*.>; in respect of the United Kingdom until 2017: section 8(4) Regulation of Investigatory Powers Act; in respect of the United Kingdom from 2017: part 6 chapter 1 Investigatory Powers Act 2016; cf. Leigh, in: Dietrich/Sule [eds.], Intelligence Law and Policies in Europe, 2019, p. 553 *et seq*.; McKay/Walker, in: Dietrich/Gärditz/Graulich/Gusy/Warg [eds.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, p. 119 *et seq*.; in respect of France: Article L854-1 to L854-9 Code de la sécurité intérieure [Des mesures de surveillance des communications électroniques internationales]; cf. Le Divelec, in: Dietrich/Sule [eds.], Intelligence Law and Policies in Europe, 2019, 516 *et seq*.; Warusfel, in: Dietrich/Gärditz/Graulich/Gusy/Warg [eds.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, p. 129 *et seq*.).

3. The comprehensive binding effect of fundamental rights on German state authority does not alter the fact that the specific protection afforded by fundamental rights can differ according to the circumstances under which they are applied. Just as this is the case for the different dimensions of fundamental rights within Germany, it is also the case for their scope of protection in other countries. The extent to which certain guarantees are applicable differs between Germany and other countries already with regard to the persons and subject matters afforded protection (see para. 196 below). Likewise, distinctions can be drawn between the different dimensions of fundamental rights – such as the effect fundamental rights have as rights against state interference, as positive obligations of the state, as decisions on values enshrined in the Constitution, or as the basis for duties of protection. Insofar as fundamental rights require further determination, the legislator may have to take into account the special circumstances abroad (cf. BVerfGE 92, 26 <41 *et seq*.>; cf. also BVerfGE 100, 313 <363>). This applies even more where the state acts in a foreign environment: this foreign environment must be taken into account when setting requirements for the justification of interferences with fundamental rights – most notably in the context of proportionality. 104

4. In the present case, the complainants assert a violation of Art. 10(1) and Art. 5(1) second sentence GG, which, as rights against state interference, afford protection 105

against surveillance measures carried out in the context of surveillance of foreign telecommunications. It follows from the fact that German state authority is in principle comprehensively bound by fundamental rights that the Federal Intelligence Service and the legislator setting out its powers are also bound by fundamental rights, at least to the extent set out above. Exempting surveillance measures by intelligence services from this binding effect of fundamental rights simply because they are directed at foreigners in other countries is alien to the Basic Law, just as exempting them from fundamental rights protection because of their political nature would be. Rather, the comprehensive binding effect of fundamental rights pursuant to Art. 1(3) GG creates the framework in which due consideration can be given to the risks to fundamental rights that arise from new technological developments and from accompanying power shifts. This applies particularly to the changing significance of intelligence services that results from advances in information technology, which allow intelligence services a wider reach in other countries.

a) The gathering of foreign intelligence by the Federal Intelligence Service has always been of considerable significance for the Federal Republic of Germany's capacity to act in the context of foreign and security policy; yet this significance has increased in recent years. In the course of internationalisation and the development of information technology, the significance and conditions under which foreign telecommunications surveillance, as a key element of foreign surveillance by the Federal Intelligence Service, is conducted have changed profoundly. 106

In the past, the only purpose of gathering foreign intelligence was the early detection of dangers to avert armed attacks on German territory; measures directly targeting individuals were limited to a small group of persons, as a result of both the technical possibilities and the intelligence interest at the time (cf. BVerfGE 67, 157 <178>). Given today's possibilities of communication and the accompanying internationalisation, potential impending dangers (*drohende Gefahren*) originating from abroad have multiplied. Information technology makes it possible to communicate directly across borders, regardless of physical distance, and to coordinate without any delay. This poses new challenges for the gathering of politically or militarily relevant communications that can be of great significance for the Federal Government's capacity to act. Moreover, today, international activities can destabilise society as a whole, as shown for example by cyber attacks, transnational organised crime such as human trafficking or money laundering, and international terrorism ([…]). Thus, gathering foreign intelligence by conducting surveillance of telecommunications is of growing importance for foreign and security policy; in political terms, this is also reflected in the budgets allocated to the intelligence services, which have increased significantly compared to many other areas (cf. the doubling of the Federal Intelligence Service's projected budget from EUR 475.5 million in 2011 […] to EUR 966.5 million in 2019 […], while the overall federal budget increased by 16% from EUR 306.8 billion to EUR 356.4 billion […]). 107

b) In the context of the tension between freedom and security, the growing importance of foreign surveillance resulting from the change in circumstances gives rise to new challenges not only for upholding security, but also for upholding freedom; a balance between these two interests must be struck in accordance with the rule of law and on the basis of fundamental rights. 108

The developments in information technology have led to a situation where data is shared through global channels, where it is randomly routed via satellite or cable according to technical criteria that have no regard to national borders (cf. on this development BTDrucks 14/5655, p. 17). This makes it possible to intercept a considerable number of foreign communications from within Germany. Moreover, communication in society has become increasingly international. In view of cross-border services, exchanges – both within states and across national borders – between citizens as fundamental rights holders mainly rely on telecommunications services that do not differentiate between domestic and foreign communications (cf. Kojm, in: Goldman/Rascoff [eds.], Global Intelligence Oversight, 2016, p. 95 <100 and 101>). Given that, under the current realities of information technology, actions and communication relations of all kinds have become increasingly digital, and given the constant increase in data processing capacities, the possibilities for conducting telecommunications surveillance extend to broad areas of all of civil society, even outside a state's own jurisdiction – just as domestic communications are also subject to surveillance by other states (cf. BTDrucks 18/12850, p. 1283 *et seq*.). 109

In light of such developments, an understanding of fundamental rights according to which their protection ended at national borders would deprive holders of fundamental rights of all protection and would result in fundamental rights protection lagging behind the realities of internationalisation ([…]). It could undermine fundamental rights protection in an increasingly important area that is characterised by intrusive state action and where – in the field of security law – fundamental rights are especially significant in general. By contrast, in binding the state as the relevant actor, Art. 1(3) GG accounts for such novel risks and helps bring them into the general framework of the rule of law that is created by the Basic Law. 110

II.

1. The challenged provisions affect the complainants' fundamental rights under Art. 10(1) and Art. 5(1) second sentence GG. The provisions authorise the collection of personal data through covert telecommunications surveillance and thus concern the guarantee of the privacy of telecommunications in Art. 10(1) GG. Accordingly, the sharing of data obtained through such measures also affects the protection afforded by the privacy of telecommunications, and such sharing must therefore also be measured against Art. 10 GG. The challenged provisions also affect the fundamental right under Art. 5(1) second sentence GG of the complainants who work as journalists. They authorise the Federal Intelligence Service to collect, process and share data from telecommunications generated in the context of these complainants' profession- 111

al activities, including targeted surveillance and analysis of their communications with journalistic sources (cf. ECtHR, Weber and Saravia v. Germany, Decision of 29 June 2006, no. 54934/00, §§ 143 *et seq*.; Big Brother Watch and Others v. the United Kingdom, Judgment of 13 September 2018, no. 58170/13 and others, §§ 476, 490 *et seq*.; see also BVerfGE 100, 313 <365>).

2. In the present proceedings, there is no need to determine whether the challenged provisions, specifically the distinction made between German citizens and EU citizens, are compatible with equality protections. In particular, it must remain unresolved whether § 6(3) BNDG, including in conjunction with § 14(2) BNDG, makes a justified distinction, because the equal treatment of German citizens and EU citizens cannot be justified by relying solely on the standards of the Basic Law, but also raises unresolved questions regarding EU law; these include the applicability of EU law in light of Art. 4(2) TEU and the fundamental freedoms and, depending on the resolution of this question, the substantive scope of the prohibition of discrimination under EU law ([…]; cf. also the pending proceedings before the CJEU, Privacy International, C-623/17, OJ EU 2018/C 022/41 [United Kingdom]; La Quadrature du Net and Others, C-511/18, OJ EU 2018/C 392/10 and French Data Network and Others, C-512/18, OJ EU 2018/C 392/11 [both France]). Thus, the Federal Constitutional Court alone cannot definitively answer the question which equality requirements the legislator must satisfy when designing a legal framework for strategic surveillance. Since the challenged provisions are unconstitutional for formal reasons alone, this question is not relevant for the proceedings. Therefore, the Federal Constitutional Court cannot refer it to the Court of Justice of the European Union. Given these circumstances, a further substantive assessment of these questions based on the Basic Law is not required either. 112

III.

The challenged provisions give rise to interferences with fundamental rights on various levels. 113

1. § 6(1) BNDG authorises the Federal Intelligence Service to intercept individual telecommunications from networks determined by a warrant; in particular, this allows for the interception of satellite signals and data transmitted via cable through the Federal Intelligence Service's own systems and also through a diversion order [addressed to telecommunications providers] pursuant to § 8 BNDG. § 14(1) BNDG authorises the Federal Intelligence Service to collect personal data in the context of cooperation with foreign intelligence services. 114

a) Such interception amounts to an interference vis-à-vis complainants nos. 1 to 7 as foreign citizens living abroad. It constitutes data collection within the meaning of constitutional law. Such interception intentionally makes the data of affected persons accessible to the Federal Intelligence Service, allowing it to analyse the data according to content-related criteria – either on the basis of search terms to identify content data, for analysing (possibly retained) traffic data or for sharing it with foreign author- 115

ities in the context of cooperation. The data that is later deleted is not just intercepted unintentionally, but is deliberately collected to analyse whether it contains relevant intelligence and, as the case may be, to use it (cf. also BVerfGE 100, 313 <366>).

b) Given the current state of technology, the same ultimately applies vis-à-vis complainant no. 8, who is a German citizen. Since § 6(4) BNDG (where applicable in conjunction with § 14(2) BNDG) does not permit surveillance measures targeting German citizens and persons within Germany, the initial interception of their data does, in principle, not amount to an interference. This data is merely intercepted unintentionally and for technical reasons; it is meant to be deleted through various filtering mechanisms after signals processing in a way that does not leave any technical traces. The interest of the authorities in this data has not taken such specific shape that the persons concerned must be considered to be directly affected in such a way that it qualifies as an interference with fundamental rights (cf. BVerfGE 100, 313 <366>; 115, 320 <343>; 150, 244 <266 para. 43>). 116

However, the current state of technology does not allow for a complete separation of data concerning German citizens and persons within Germany, meaning that in some cases such data is included in the analysis. It is then only deleted once the relevant data is identified during manual screening. While it is not clearly ascertainable that § 6(1) and (4) BNDG permits this approach, such an understanding of the provision is required in order to be able to apply it at all; this is also how it is understood in practice. This amounts to an interference in relation to persons whose data is intercepted in this manner, without being deleted after signals processing in a way that does not leave any technical traces, and whose data is thus viewed by Federal Intelligence Service staff. As § 6(1) and (4) BNDG provides the statutory basis for this approach, it amounts to an authorisation to interfere with the fundamental right under Art. 10(1) GG in relation to complainant no. 8 as well. 117

2. § 6(1) to (3) BNDG gives rise to further interferences with the complainants' fundamental rights as it authorises further analysis of the data. Firstly, § 6(1) BNDG and, to the extent set out in that provision, § 14(1) BNDG in conjunction with § 19(1) BNDG authorise an interference in the form of analysis of the telecommunications traffic data that was collected, including the data stemming from traffic data retention. Secondly, § 6(1) to (3) BNDG authorises the analysis of intercepted telecommunications by means of search terms for the purpose of screening content data. The provision also authorises manual screening of the telecommunications identified through analysis, which encompasses further data processing – ranging from screening telecommunications selected through search terms to decoding and forwarding them to the relevant departments for further use – and also amounts to further interferences. 118

3. A separate interference with fundamental rights lies in the potential sharing of intelligence obtained through surveillance, to the extent that it contains personal data, which is provided for under various separate constituent elements in § 24 BNDG. In 119

the context of intelligence sharing, the data obtained is made accessible to other authorities, which qualifies as a separate interference with fundamental rights with regard to each instance of sharing (cf. BVerfGE 141, 220 <324 and 325 para. 279>). Accordingly, the automated sharing of information with foreign authorities, as provided for by § 15(1) BNDG in the context of cooperation, amounts to an interference with fundamental rights.

4. § 7 BNDG also gives rise to interferences with Art. 10(1) GG and, where applicable, Art. 5(1) second sentence GG. While this provision itself does not provide for the collection of data through surveillance measures but merely presumes that such collection takes place ([…]), § 7(1) BNDG provides a basis for further processing the data thus obtained, which amounts to a separate interference (cf. BVerfGE 100, 313 <366 and 367>). Moreover, § 7(2) BNDG sets out restrictions regarding data collection, thus making data collection from abroad appear permissible even in the absence of any further statutory basis. Ultimately, § 7(1) and (2) BNDG aims to provide legitimation for data collection conducted by the Federal Intelligence Service from abroad. 120

D.

These interferences with fundamental rights are not justified under constitutional law. For formal reasons alone, the provisions authorising these interferences do not satisfy the constitutional requirements for statutory bases authorising interferences with the affected fundamental rights. While they are based on a legislative competence that is sufficient, they violate the requirement to expressly specify affected fundamental rights (*Zitiergebot*), which is enshrined in Art. 19(1) second sentence GG. 121

I.

There are no major constitutional concerns with regard to legislative competence. The federal legislator was competent to enact the challenged provisions on the basis of Art. 73(1) no. 1 GG. 122

1. […] 123

a) It is undisputed that the establishment of an agency responsible for comprehensive foreign surveillance is covered by the competence for foreign affairs within the meaning of Art. 73(1) no. 1 GG (cf. BVerfGE 100, 313 <369>). This also includes the conferral of powers that are required to carry out such tasks. However, the legislator can only assign certain tasks to such an agency. 124

aa) The meaning of foreign affairs in Art. 73(1) no. 1 GG cannot be determined without considering the overall division of legislative competences. […] 125

[…] 126

bb) The Federation cannot task the Federal Intelligence Service with foreign surveillance for national security purposes in general. Art. 73(1) no. 1 GG does not entitle the federal legislator to grant powers that are aimed at preventing, averting or prose- 127

cuting criminal acts as such (cf. BVerfGE 100, 313 <370>; 133, 277 <319 para. 101>). It can only confer tasks and powers on the Federal Intelligence Service that are significant to foreign and security policy and thus have an international dimension.

Yet this does not limit the federal legislator to tasking the Federal Intelligence Service with providing intelligence to the Federal Government for the purpose of safeguarding its capacity to act in matters of foreign and defence policy (cf. BVerfGE 100, 313 <368 *et seq*.>). It is true that this is the primary function of foreign surveillance, which must remain central to the overall profile of an intelligence service established on the basis of Art. 73(1) no. 1 GG. However, the Federal Intelligence Service can also be tasked with the separate responsibility of early detection of impending dangers originating from abroad if these dangers are sufficiently international in scope. It is decisive that these dangers be of such nature and gravity that they can affect the position of the Federal Republic of Germany in the international community and that they be significant to foreign and security policy precisely for this reason. […] 128

b) [...] 129-131

2. […] 132-133

II.

However, the challenged provisions are formally unconstitutional since they violate the requirement to expressly specify affected fundamental rights, which is enshrined in Art. 19(1) second sentence GG ([…]). The Federal Intelligence Service Act refers to Art. 10(1) GG in relation to interferences resulting from § 3 BNDG (cf. § 3(3) BNDG), but not in relation to interferences resulting from the provisions at issue here. Failure to adhere to the requirement to expressly specify affected fundamental rights cannot be justified by the fact that the challenged provisions enshrine into law a long-standing administrative practice for the first time. In particular, it cannot be claimed that the requirement to expressly specify affected fundamental rights does not apply if the law provides for fundamental rights restrictions that already exist in prior legislation or only provides for minor deviations from them (cf. on this BVerfGE 35, 185 <188 and 189>). Administrative practice that lacks a legal basis constitutes neither applicable law nor a valid restriction of fundamental rights; unlike acts of Parliament that adhere to the requirement to expressly specify affected fundamental rights, such practice is not based on value decisions made by the parliamentary legislator. Nor can mere administrative practice serve as a warning that is equivalent to the one provided by [a law adhering to] the requirement to specify affected fundamental rights. This holds true all the more for the covert practice of an intelligence service. 134

The legislator violates the requirement to specify fundamental rights precisely where it considers these fundamental rights to be unaffected based on a certain interpretation of their scope of protection – in this case, the assumption that German state au- 135

thority is not bound by fundamental rights when acting abroad in relation to foreigners. In such a case the legislator is not aware that it authorises interferences with fundamental rights and is not willing to account for their consequences, yet this is the very purpose of the requirement to specify affected fundamental rights (cf. BVerfGE 85, 386 <404>; 113, 348 <366>; 129, 208 <236 and 237>). Moreover, the legislator thus evades a public debate, which would serve to clarify the necessity and scale of interferences with fundamental rights (cf. BVerfGE 85, 386 <403 and 404>; 129, 208 <236 and 237>).

E.

In substantive terms, too, the challenged provisions are not compatible with the Basic Law. While the Basic Law does not generally preclude the use of strategic surveillance and the cooperation with other intelligence services relating thereto, the challenged provisions do not satisfy the key requirements arising from fundamental rights. 136

I.

1. Like any interference with fundamental rights, interferences with Art. 10(1) GG and Art. 5(1) second sentence GG must be based on a statutory authorisation that satisfies the requirements of legal clarity and specificity (cf. BVerfGE 65, 1 <44; 54>; 100, 313 <359 and 360>; established case-law). Provisions authorising the covert collection and processing of personal data are generally subject to more stringent requirements regarding legal clarity and specificity; this is because affected persons are not aware that their data is being processed and these powers can thus not be specified incrementally through individual warrants issued by the relevant authorities combined with judicial review (cf. BVerfGE 141, 220 <265 para. 94>; cf. also ECtHR, Big Brother Watch and Others v. the United Kingdom, Judgment of 13 September 2018, no. 58170/13 and others, § 306). 137

Intelligence services are not exempt from these requirements. It is true that they must largely perform their tasks covertly. Especially surveillance carried out abroad must generally be strictly shielded from public knowledge so as to be able to obtain intelligence without jeopardising one’s own resources and sources (cf. BVerfGE 30, 1 <18 and 19>; 100, 313 <397 and 398>). In this respect, not only specific measures carried out and intelligence obtained by the Federal Intelligence Service, which is tasked with these functions, must be kept secret, but also the extent to which the intelligence service can or cannot obtain intelligence on certain questions and the level of detail of such intelligence. Since the intelligence service must assume that foreign services will try to spy on it, these secrecy requirements extend deep into the structure of intelligence services. The legislator may take this into account. 138

However, it cannot be inferred from the need to keep foreign surveillance secret that as little as possible should be known about the Federal Intelligence Service itself or that its statutory bases must largely remain undisclosed. In a democratic state under the rule of law, there can be no general secrecy as to the statutory bases for intelli- 139

gence activities and the limits of intelligence powers. Just as the overall budget and the number of staff of intelligence services are entirely determined by Parliament and are subject to public accountability (regarding scrutiny of the detailed use of funds cf., by contrast, § 10a of the Federal Budget Code, *Bundeshaushaltsordnung* – BHO), their powers, too, must be openly determined by law in a clear and specific manner and it must be clearly set out to whom they are accountable ([…]). As the state is bound by fundamental rights, it has parliamentary and democratic responsibility for restricting fundamental rights. Thus, intelligence services can only act covertly in accordance with publicly accessible law. Even for foreign surveillance, secrecy is not an end in itself; rather, it is only justified if the type and extent of the intelligence service's activities requiring secrecy are democratically and publicly legitimated and if secrecy remains within the specific limits of functional necessity.

The requirement of clear and sufficiently specific statutory powers of intelligence services does not call into question the possibility of keeping the intelligence obtained through such powers secret. Given that the powers only create abstract legal possibilities, they allow no conclusions to be drawn as to whether, how, to what extent and how successfully intelligence services make use of them. 140

2. To the extent that the challenged provisions authorise interferences with the privacy of telecommunications and freedom of the press, they can only be justified if they satisfy the principle of proportionality. According to this principle, they must have a legitimate purpose and must be suitable, necessary and proportionate in the strict sense for achieving that purpose (cf. BVerfGE 67, 157 <173>; 120, 378 <427>; 141, 220 <265 para. 93>; established case-law). The Federal Constitutional Court has specified the standards deriving from proportionality in several decisions concerning covert surveillance measures carried out by security authorities and summarised them particularly in the decision on the Federal Criminal Police Office Act (cf. BVerfGE 141, 220 <268 *et seq*. para. 103 *et seq*.>). These standards also apply to surveillance measures carried out by the intelligence services; they form the basis both for the requirements regarding data collection and processing and for the requirements regarding data sharing. However, the instrument of strategic surveillance as a special means of gathering foreign intelligence is not specifically considered within these standards. Therefore, they must be specified, in line withthe decision on strategic surveillance powers under the Article 10 Act (cf. BVerfGE 100, 313 <368 *et seq*.>). 141

II.

The powers to collect and process data in the framework of strategic telecommunications surveillance as a special instrument for gathering foreign intelligence are compatible with Art. 10(1) GG in principle (see 1. below). Yet the legal provisions must set out sufficient restrictions in relation to these powers (see 2. below). 142

1. Art. 10(1) GG does not, from the outset, rule out creating powers to gather foreign intelligence by means of strategic telecommunications surveillance. While the use of 143

these powers is not limited to specific and objectively determined grounds and creating these powers thus authorises serious interferences with fundamental rights without any thresholds for their use, these powers, if sufficiently restricted, may still be justified in light of Art. 10(1) GG and the principle of proportionality by the aim of foreign surveillance and the special conditions under which it is conducted.

a) Strategic telecommunications surveillance serves a legitimate purpose and, in accordance with the principle of proportionality, is suitable and necessary for achieving that purpose. According to the legislative intent, strategic surveillance is meant to yield intelligence on foreign matters that are significant to the foreign and security policy of the Federal Republic of Germany. It thus serves to contribute to the early detection of dangers, to safeguarding the Federal Republic of Germany's capacity to act and to providing information to the Federal Government on matters of foreign and security policy. This constitutes a legitimate aim. Strategic telecommunications surveillance is a suitable means for achieving that aim, because it makes it possible to obtain such information. Even though large volumes of data are initially intercepted that have no relevant informative value, this does not alter the fact that the comprehensive interception and analysis of data can ultimately yield significant intelligence. Strategic surveillance also satisfies the requirements for necessity. Without broad interception and analysis of data that is not based on specific grounds, such intelligence could not be obtained. No less intrusive means that would yield generally comparable intelligence are available. 144

b) Authorising the Federal Intelligence Service to carry out strategic surveillance of foreign telecommunications can, in principle, also be justified in light of Art. 10(1) GG with regard to proportionality in its strict sense. 145

aa) However, strategic telecommunications surveillance results in interferences of particularly great weight. 146

(1) The interferences are of such great weight because this instrument is used to covertly intrude into personal communications, which are often private and in some cases even highly confidential. Such covert surveillance of telecommunications generally amounts to a serious interference (cf. BVerfGE 141, 220 <264 and 265 para. 92>), regardless of whether surveillance is conducted from within Germany or from abroad and whether it targets persons within Germany and German citizens or foreign citizens abroad. 147

(2) Yet compared to targeted surveillance of individual telecommunications, strategic surveillance gives rise to interferences of less weight given that it relates to data whose informative value cannot be foreseen in detail. To the extent that strategic surveillance targets individuals by means of formal search terms, it is typically less precise and not as comprehensive, given that the networks and transmission routes (so-called routing) used for a specific communication link are largely determined spontaneously depending on availability and given that only a fraction of the networks existing in Germany and internationally are covered by bulk interception warrants. At 148

least in principle, the weight of interference resulting from strategic surveillance must be distinguished from the weight of interference resulting from restrictions in specific cases, as provided for by § 3 of the Article 10 Act.

(3) Moreover, its weight of interference vis-à-vis persons abroad is lower because this form of surveillance is not aimed at immediate operational consequences in the same manner as surveillance measures targeting Germans or persons within Germany. Foreign surveillance concerns acts in other countries, where the German state is not vested with sovereign powers, and it is the exclusive responsibility of the Federal Intelligence Service, an authority that generally does not have its own operational [police] powers. The primary role of foreign surveillance is to create an informational basis, evaluate the information obtained, assess its relevance and make it available, in an edited form, to the Federal Government and, as the case may be, other recipients. However, one of the aims of such surveillance is often to take action against individuals – possibly even through sharing intelligence with other states; therefore, it is a serious interference nonetheless. Yet the Federal Intelligence Service itself cannot take such action against individuals abroad. Where other bodies take action against individuals based on such information, they have to rely on the sharing of data, which can, and must, be restricted by the principle of hypothetical recollection of data (see paras. 216, 217 and 220 *et seq*. below). 149

(4) By contrast, the exceptionally broad scope and the indiscriminate effect of strategic telecommunications surveillance is particularly aggravating. Such surveillance can be used against anyone without requiring specific grounds; it is merely restricted by the specific purposes pursued. Objective thresholds for the use of this power are not required, neither with regard to the situations in which surveillance measures are permissible nor with regard to the individuals affected by them. As long as it stays within the boundaries of the purposes of surveillance measures, which are only determined in the abstract, the authority vested with such powers can freely decide which networks, data and individuals it wants to target. 150

Such powers have an exceptional reach, particularly given the realities of modern information technology and its significance for communication relations. As regards the intensity of interference resulting from these powers, they cannot be compared to the powers [under the Article 10 Act] in respect of which the Federal Constitutional Court rendered a decision in 1999 concerning strategic surveillance measures targeting international communications (where one communicating party is in Germany and the other is abroad; *Inland-Ausland-Kommunikation*). At the time, telecommunications surveillance was *de facto* restricted to narrowly defined means of telecommunication that were solely used in specific situations (cf. BVerfGE 100, 313 <379 and 380>), whereas today the volume of intercepted data alone is exponentially larger. The data flows targeted by surveillance carry an immense volume of electronic telecommunications, which are then analysed. Given the ubiquitous and diverse use of communication services, all forms of activity of individuals and of human interaction are increasingly reflected in electronic signals and thus become a potential target 151

of telecommunications surveillance. Thus, surveillance covers communications reaching deep into everyday life, including highly private and spontaneous communications and the sharing of images or files. […]

(5) Strategic telecommunications surveillance gives rise to interferences of particular weight insofar as it also allows for targeted surveillance of specific individuals. Surveillance thus acquires a new dimension that did not exist with regard to the powers reviewed by the Court in its decision in 1999 [concerning the Article 10 Act]. The strategic surveillance measures examined in that decision used content-related search terms, but were not linked to specific individuals (cf. BVerfGE 100, 313 <384>). By contrast, the strategic surveillance measures at issue in the present case mostly use formal search terms such as telecommunications identifiers, which make it possible to target specific individuals. Thus, strategic telecommunications surveillance gives rise to interferences that are fundamentally more far-reaching and more closely resembles targeted telecommunications surveillance. 152

(6) Compared to the previous legal framework, an aggravating factor is that, to a certain extent, strategic surveillance now also allows for traffic data to be retained in its entirety. The analysis of such traffic data – without specific grounds and merely guided by the purpose pursued – can provide deep insights into the communication behaviour and movement patterns of the affected persons, which may go far beyond the content-based analysis of individual communications (cf. regarding the informative value of such data BVerfGE 125, 260 <319>; CJEU, Judgment of 8 April 2014, Digital Rights Ireland and Seitlinger and Others, C-293/12, C-594/12, EU:C:2014:238, paras. 48, 56). This, too, considerably increases the weight of interference. 153

bb) As specific powers for gathering foreign intelligence, strategic surveillance powers can be justified under constitutional law, despite the particularly serious weight of interference resulting from such surveillance. 154

(1) Yet by refraining from creating specific thresholds for the use of powers, the legislator fails to satisfy a core requirement arising from the rule of law. Such thresholds are indispensable in general, and are of even greater importance in respect of domestic security authorities, even for less intrusive interferences with fundamental rights, but certainly for serious interferences such as telecommunications surveillance (cf. BVerfGE 141, 220 <269 *et seq*. para. 104 *et seq*.>; 150, 244 <280 *et seq*. para. 90 *et seq*.>). The requirement of thresholds tied to specific circumstances ensures that interferences with fundamental rights are restricted, makes them contingent upon objective requirements and allows for oversight based on independent criteria. An authorisation of such interferences that is solely guided and restricted by the purpose pursued is generally incompatible with Art. 10(1) GG. 155

In principle, this also applies to intelligence services. Insofar as surveillance measures extend to domestic communications, reliable thresholds are required in accordance with the general requirements. The same holds true for surveillance measures 156

ordered by targeted warrants against specific individuals – whether they are in Germany or abroad –, for instance telecommunications surveillance measures or remote searches [of information technology systems] (cf. BVerfGE 120, 274 <326 *et seq*.>; 125, 260 <320 *et seq*.>; 141, 220 <270 *et seq*. para. 106 *et seq*.>; see also § 3 of the Article 10 Act).

(2) By contrast, the gathering of foreign intelligence by intelligence services is treated differently insofar as it is aimed at providing general information to the Federal Government or – prior to restrictions of an individual's [fundamental right under Art. 10 GG] – at the early detection of dangers. In these areas, the legislator may confer upon the Federal Intelligence Service the power to carry out strategic telecommunications surveillance. The fact that essentially such surveillance is only guided and restricted by the purpose pursued is not from the outset incompatible with the proportionality requirements (on the strategic surveillance of international telecommunications BVerfGE 100, 313 <373 *et seq*.>). 157

(a) In this respect, the specific tasks that form part of foreign surveillance must be considered. Its primary aim is not to carry out targeted investigations of acts that have already been established and thus to gather information on clearly defined situations; rather, it mainly serves to detect and identify relevant information regarding intelligence interests that can only be defined in abstract terms. Thus, the role of foreign surveillance is to create a comprehensive informational basis, observe a broad range of developments, evaluate the information obtained, assess its relevance and make it available, in a condensed form, to the Federal Government and, as the case may be, other recipients. Given that potential intelligence interests concern the entire field of foreign and security policy, they relate to a wide range of information. 158

(b) In respect of this task, strategic surveillance without specific grounds that is essentially guided solely by the purpose pursued can be justified under constitutional law. In contrast to measures for the early detection of domestic dangers, it is significant that foreign surveillance is aimed at understanding and providing information about circumstances which cannot be directly perceived on a daily basis by German bodies or the German public. Its purpose is to yield intelligence regarding developments in contexts that are difficult to interpret on the basis of domestically obtained information only and that in part concern countries whose openness in terms of information structures is limited. Yet above all, the special conditions under which this task must be performed are decisive. Foreign surveillance concerns occurrences in other states, where the German state generally has no or only few resources for gathering intelligence and where it is not vested with sovereign powers granting it direct access to information (cf. also ECtHR, Big Brother Watch and Others v. the United Kingdom, Judgment of 13 September 2018, no. 58170/13 and others, § 518). In the interest of the Federal Republic of Germany's security and capacity to act, the intelligence that can be obtained must also include information that is deliberately withheld from Germany – possibly with negative intentions – and is kept secret within the other jurisdiction. Under the law of the state targeted by surveillance measures, such mea- 159

sures may also be illegal, or at least unwanted. The intelligence service may then be faced with defences of the targeted states, which use their police and intelligence services to obstruct and undermine surveillance. Therefore, the work is particularly exposed and precarious, requiring extraordinary means.

It must also be taken into account that surveillance is not solely characterised by different intelligence services working against each other; instead, these services also cooperate to gather intelligence on matters concerning both the Federal Republic of Germany and other countries. Effective surveillance requires cooperation between intelligence services, particularly where surveillance solely aims to provide information to the Federal Government regarding political or military scenarios, but also where its aim is the early detection of dangers posed by international crime, including international terrorism. However, the Federal Intelligence Service is only able to engage in such cooperation if it also has the powers to examine the intelligence gathered by other services, to use and further analyse foreign intelligence, and if it can use its powers to contribute intelligence as a partner. Based on current knowledge, intelligence services in other countries will commonly have powers to carry out surveillance of foreign telecommunications without specific grounds (in respect of the United States: Section 702 Foreign Intelligence Surveillance Act; cf. Renan, in: Goldman/Rascoff [eds.], Global Intelligence Oversight, 2016, p. 121 <particularly 123 *et seq*.>; in respect of the United Kingdom: part 6 chapter 1 Investigatory Powers Act 2016; cf. Leigh, in: Dietrich/Sule [eds.], Intelligence Law and Policies in Europe, 2019, p. 553 *et seq*.; McKay/Walker, in: Dietrich/Gärditz/Graulich/Gusy/Warg [eds.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, p. 119 *et seq*.; in respect of France: Article L854-1 to L854-9 Code de la sécurité intérieure [Des mesures de surveillance des communications électroniques internationales]; cf. also Le Divelec, in: Dietrich/Sule [eds.], Intelligence Law and Policies in Europe, 2019, p. 516 *et seq*.; Warusfel, in: Dietrich/Gärditz/Graulich/Gusy/Warg [eds.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, p. 129 *et seq*.). 160

(c) The exceptionally significant public interest in the effective gathering of foreign intelligence must also be taken into account. 161

In line with the legislative competence for conferring powers to conduct foreign surveillance (see para. 123 *et seq*. above), such surveillance is always aimed at yielding information that is significant for Germany's position and capacity to act within the international community and, in that sense, is significant to foreign and security policy. The provision of information to the Federal Government for its decision-making on foreign and security policy helps it to assert itself in the realm of international power politics and can prevent erroneous decisions leading to potentially serious consequences. This indirectly bears on the safeguarding of democratic self-determination and the protection of the constitutional order – and thus on high-ranking constitutional interests. What is at issue here is an interest of the nation as a whole, which significantly goes beyond the interest in guaranteeing national security as such. 162

It is important to note that threats originating from abroad have increased significantly as part of the advances in information technology and international communication as well as the closer interconnectedness of living conditions across borders. In this context, the early detection of dangers originating from abroad takes on particular importance for public security. The expansion and internationalisation of the possibilities for conducting communication and the resulting increased politicisation and ability to organise of international criminal gangs mean that domestic situations of danger frequently originate in networks of actors cooperating internationally with foreign and security policy dimensions. The challenges posed by globally connected groups engaging in organised crime, money laundering, human trafficking, electronic attacks on information technology systems, international terrorism and the trade in weapons of war clearly illustrate this point (cf. Kojm, in: Goldman/Rascoff [eds.], Global Intelligence Oversight, 2016, p. 95 *et seq*.; Goodman/Ischebeck-Baum, in: Dietrich/Sule [eds.], Intelligence Law and Policies in Europe, 2019, p. 1 <esp. para. 104 *et seq*.>; regarding dangers of cyber crime see also BTDrucks 18/4654, pp. 40 and 41; regarding dangers posed by international terrorism and weapons proliferation see already BTDrucks 12/6853, pp. 20, 42). Some of these activities seek to destabilise society (regarding international terrorism cf. BVerfGE 115, 320 <357>; 133, 277 <333 and 334 para. 133>; 143, 101 <138 and 139 para. 125>) and can jeopardise the constitutional order, the existence and security of the Federation and of the *Länder* and life, limb and liberty. These are legal interests that are exceptionally significant under constitutional law, and the legislator may consider effective foreign surveillance, circumscribed in accordance with the rule of law, to be an indispensable means for protecting these interests (cf. BVerfGE 115, 320 <358>; 143, 101 <138 and 139 para. 124 *et seq*.>). 163

Consequently, the disproportionately broader access to data that is permitted in the context of strategic surveillance today is matched by a higher potential for danger than in the case [concerning the Article 10 Act] decided by the Federal Constitutional Court in 1999. For this reason, Art. 10(1) GG and the proportionality requirements resulting therefrom in principle do not preclude the use of search terms targeting specific individuals for strategic surveillance measures. This is also why the law may, generally and to a limited extent, provide for the retention of the entirety of traffic data and for subsequent analysis of this data without requiring specific grounds for doing so. 164

(d) An important aspect supporting the argument that strategic telecommunications surveillance is justifiable is that the consequences of undertaking such surveillance without specific grounds are somewhat mitigated by the fact that it is conducted by an authority that, in principle, has no operational powers itself. Given the actual circumstances of cases concerning intelligence on persons located in other countries, such intelligence can generally not lead to direct follow-up measures against them, as German authorities are not vested with sovereign powers when acting abroad. However, this does not call into question that surveillance measures carried out 165

abroad can also give rise to serious consequences for affected persons, and that such measures also serve to provide a basis for follow-up measures against these persons – either through data sharing or when the persons concerned subsequently cross the border. Yet given that the data is collected by an authority that in principle has no operational powers itself, any further use of this data depends on a screening of the data carried out by persons that have no responsibility for operational action themselves. Therefore, sharing this data for operational use can, and must, be subjected to qualified thresholds (see para. 220 *et seq*. below).

c) Based on the above considerations, the instrument of strategic surveillance, including the use of formal search terms targeting specific individuals and the collection and analysis of traffic data, sometimes in its entirety, is not in principle incompatible with Art. 10(1) GG or the proportionality requirements resulting therefrom. However, given that they are not based on specific grounds and essentially guided and restricted only by the purpose pursued, the powers to conduct strategic surveillance are exceptional powers that must be restricted to foreign surveillance conducted by an authority that itself has no operational powers for averting dangers to public security. These powers can only be justified by the authority's particular tasks and the specific conditions under which these tasks are performed. In accordance with the principle of proportionality, the specific design of the surveillance powers must be in line with these considerations. 166

2. The legislative design of data collection and processing in the framework of strategic surveillance is subject to further requirements, which must take into account the particular weight of the interferences with fundamental rights and the specific justification provided by the particular task and conditions of foreign surveillance. 167

a) An overarching aim of the requirements arising from the principle of proportionality is to limit strategic telecommunications surveillance by ensuring that it is designed as a sufficiently focussed instrument despite its broad scope and indiscriminate effect. The Basic Law does not allow for global and sweeping surveillance, not even for the purpose of gathering foreign intelligence (cf. BVerfGE 100, 313 <376>). 168

Therefore, the legislator must restrict the volume of data to be taken from the respective transmission channels ([…]) and the geographical area covered by surveillance. Since the technical possibilities for processing data are changing quickly, merely referring to actual capacity limits in this respect is insufficient ([…]). Yet above all, the legislator must circumscribe the powers in accordance with the rule of law so as to structure and partially restrict data collection and processing. In particular, this includes rules on the use of filtering techniques (see b) below), the purposes of surveillance (see c) below), the design of the surveillance process (see d) below), the focused use of search terms (see e) below), the limits of traffic data retention (see f) below), the methods of data analysis (see g) below), the protection of relationships of trust (see h) below) and the protection of the core of private life (see i) below), as well as the imposition of obligations to delete data (see j) below). In addition, the legislator 169

must adhere to requirements regarding transparency, individual legal protection and, above all, comprehensive independent oversight (for general considerations on this, see V. below).

b) Given that strategic surveillance can only be justified as an instrument for gathering foreign intelligence, further data processing must be based on clear provisions requiring that data stemming from domestic communications be removed. 170

aa) Provisions on the removal of data stemming from telecommunications in which Germans or persons within Germany are involved on both sides are required in any case, since, in this constellation, telecommunications surveillance that is not based on specific grounds is impermissible from the outset. 171

Once domestic communications have been removed, strategic surveillance measures can be aimed at two things: firstly, the surveillance of communications designated as “international” in § 5 of the Article 10 Act (communications where one communicating party is located within Germany and the other is abroad, *Inland-Ausland-Kommunikation*), and, secondly, the surveillance of exclusively foreign communications (where all communicating parties are abroad, *Ausland-Ausland-Kommunikation*). Both types of surveillance must be measured against Art. 10(1) GG in the same way. In certain respects, however, the surveillance of communications between two foreign interlocutors results in interferences of lesser weight than the surveillance of international communications between an interlocutor abroad and a domestic interlocutor, given that the latter intercepts communications that are directly linked to domestic matters and thus reaches deeper into the domestic legal order. This is why the surveillance of foreign telecommunications is, in some respects, subject to less strict requirements (cf. para. 177 below regarding the possibility of gathering intelligence irrespective of dangers in order to provide information to the Federal Government; cf. paras. 179 and 180 below regarding the possibility of selecting the search terms only after the [purposes and duration of the] surveillance measure have been determined; cf. paras. 254 *et seq*. and 262 *et seq*. below regarding automated sharing of data with foreign intelligence services in the context of cooperation). If the legislator wants to take into account the differing weight of the interferences arising from the two types of surveillance measures in question and if it therefore wants to provide for different legal provisions, it must require the deletion of international communications, too. 172

bb) The requirements regarding the removal of domestic and international communications must be set out in clear provisions. As far as technically possible, automated filters must be used to ensure that the Federal Intelligence Service’s staff does not obtain knowledge of such telecommunications data. The indiscriminate interception of all data, including domestic data, by the Federal Intelligence Service’s systems is not impermissible from the outset as long as it is technically unavoidable. However, in that case the legislator must enact clear provisions requiring that data stemming from domestic communications and, as the case may be, international communica- 173

tions be technically separated and deleted without any trace, using any means available, before the data is manually analysed. The legislator must impose an obligation on the intelligence service to continually develop filtering methods and to keep them up to date with developments in science and technology.

Where such filtering cannot fully guarantee that the data is separated, the further use and analysis of the prefiltered data is not precluded. Yet the law must then ensure that, in the event of telecommunications data of Germans or persons within Germany being identified in the context of further analysis, this data is deleted immediately without being used. The legislator may only provide for an exemption insofar as the data in and of itself indicates an immediate and specific danger (*unmittelbar bevorstehende konkrete Gefahr*) to life, limb or liberty of the person, vital interests of the public or the existence or security of the Federation or of a *Land*. Directions in an internal manual referring to general principles of criminal law are not sufficient to justify such a power (in contrast to this, cf. 3.9 of the SIGINT Manual); rather, an explicit statutory provision is required. Such use may have to be documented (see para. 291 below) and requires oversight that resembles judicial review. 174

c) Moreover, the legislator must determine the purposes of telecommunications surveillance and of the use of intelligence thus obtained in sufficiently clear and specific statutory provisions (cf. BVerfGE 100, 313 <372>). 175

aa) Given that telecommunications surveillance is a particularly intrusive instrument for gathering foreign intelligence, it must be substantially restricted to sufficiently limited and precisely defined purposes, for which the legislator is responsible. Within the limits of the relevant legislative competences, the purposes that can be taken into consideration are those that aim to protect high-ranking interests of the common good, the violation of which would result in serious harm to external and domestic peace or to the legal interests of individuals (cf. BVerfGE 100, 313 <373>). 176

bb) In contrast to this, measures carried out in the context of surveillance of foreign telecommunications that are, from the outset, only aimed at providing information to the Federal Government to prepare governmental decisions can be permissible even if they are not aimed at the early detection of dangers. To this end, the legislator may provide for surveillance measures for the entire range of tasks performed by the Federal Intelligence Service. It may, for example, tie these measures merely to orders of the Federal Government – yet the legislator must restrict them, in line with its legislative competences, to measures concerning foreign and security policy. However, if the legislator does so, it must ensure that a change in the purpose for which the data may be used is excluded in principle and that the intelligence obtained through such surveillance not be shared with other bodies (see para. 223 *et seq*. below), aside from special exemptions (see para. 228 below). 177

d) Insofar as they are used to pursue the purposes defined by law, the legislator may in principle permit strategic surveillance measures without requiring specific grounds and does not have to tie them to objective thresholds (see para. 157 *et seq*. 178

above). Yet as the powers to conduct strategic surveillance is only guided by the purpose pursued, the legislator must set out procedural safeguards adequately ensuring that the powers are based on the respective purposes and thus also allow for oversight ([…]).

aa) The granting of such powers must be based on a formal determination of precisely defined surveillance measures. This amounts to a designation of the specific purpose of the measure within the meaning of data protection law. As a basis for justifying such a measure vis-à-vis the persons under surveillance, the determination must specify the aims and duration of the measure. Generally, it must include the type of danger on which intelligence is to be obtained and the geographic focus of surveillance. The measures must be limited in time. This does not rule out that they may be extended, even repeatedly. 179

Under constitutional law, the legislator is not restricted to a specific approach for the internal procedural design of such formal determinations. The legislator can choose from various organisational arrangements and may also have to consider – possibly depending on the different types of communications subjected to surveillance – prior authorisation by the head of the Federal Intelligence Service or the involvement of the Federal Chancellery. Insofar as the legislator limits strategic surveillance to data stemming from foreign communications only, an involvement of institutions with direct political accountability is not always necessary. Moreover, the search terms do not in every case have to be specified in advance, i.e. in the context of the determination of the measure (cf. regarding the Article 10 Act BVerfGE 100, 313 <373 and 374>). 180

Yet in line with the prior judicial authorisation required for telecommunications surveillance targeting individuals that is authorised by an individual warrant (cf. BVerfGE 125, 260 <337 and 338>; 141, 220 <312 para. 235>), the determination of a strategic surveillance measure as such requires oversight that resembles judicial review. While it must in principle be ensured that such oversight is conducted before the measure is carried out, exemptions in cases of urgency are not ruled out. 181

bb) The purposes of the surveillance measures that are defined in this manner must be used to determine the further procedure for data collection and processing, which must subsequently be accessible to independent oversight. This concerns both the selection of the transmission channels necessary for the surveillance measure in question, which are to be subject to restrictions [of Art. 10 GG] and are to be intercepted for analysis, and the selection of search terms. These purposes are also decisive for labelling and using the data. Rules for the use of coincidental findings made possible by internal changes in purpose are permissible nonetheless (cf. BVerfGE 141, 220 <326 *et seq*. para. 284 *et seq*.>). 182

dd) It will not be possible to limit the surveillance measures that are determined in a differentiated manner, as set out above, to a few measures. Based on current practice, which is structured differently, representatives of the Federal Intelligence Service estimated in the oral hearing that there are approximately 100 to 200 different 183

surveillance interests or intelligence perspectives that are handled separetely. This number may be reduced somewhat when these perspectives are combined, as set out above, to form coherent but sufficiently precise and delimited categories of surveillance measures. Yet structuring surveillance measures in such a way serves to create a clear and sufficiently differentiated profile for the respective surveillance measures so as to guide the collection and analysis of data in detail. It is therefore adequate that the number of surveillance measures determined in this manner is significantly higher than the number of bulk warrants that exist under current practice, of which there are currently 17 (see para. 16 above).

Under constitutional law, this does not rule out that bulk warrants and warrants ordering telecommunications providers to divert communications based thereon can be issued together to carry out a larger number of different surveillance measures. From a technical perspective, cross-checking intercepted data against the search terms assigned to the different measures can be carried out in the same setting; the resulting matches can then be reassigned to the respective measures in a subsequent step. Constitutional law does not require that the Federal Intelligence Service follow any specific approach for the organisation of such technical procedures. 184

e) Strategic surveillance gives rise to interferences of particular weight given that it predominantly uses formal search terms and thus also targets specific individuals. This is not generally impermissible under constitutional law. Nonetheless, restrictions are required that, in accordance with the principle of proportionality, take into account the affected persons' need for protection. 185

aa) In line with current practice, the targeted interception of telecommunications of German citizens must be ruled out. This applies both to the surveillance of international communications (cf. § 5(2) of the Article 10 Act) and to the surveillance of foreign communications. It is true that Art. 10(1) GG equally protects foreigners and Germans and that the strategic surveillance of telecommunications gives rise to serious interferences with fundamental rights vis-à-vis both groups. However, this does not call into question that, in the individual case, the weight of interference resulting from such surveillance differs vis-à-vis the two groups; this must be reflected in the design of the statutory bases authorising interferences. Generally, the weight of interference resulting from surveillance is greater vis-à-vis German citizens than vis-à-vis foreigners in other countries because German citizens are within the reach of German authorities to a far greater extent and can thus more easily be subjected to follow-up measures. Above all, this holds true for Germans that are staying in other countries only for a short period of time. Yet in principle, this applies to all German citizens, given that they are subject to the personal jurisdiction of the Federal Republic of Germany, even if they live abroad for a longer period of time; they are also dependent on contact with German authorities – at least to fulfil their obligations under the law relating to identification and identity cards –, and it can be assumed that most of them will have closer ties to Germany and enter the country more often than foreign citizens. Therefore, in the context of strategic surveillance, the targeted surveil- 186

lance of telecommunications of German citizens that is not based on specific grounds is of such weight as to make the resulting interferences with Art. 10(1) GG appear disproportionate. The targeted surveillance of telecommunications of German citizens must thus be subject to the requirements that apply to the individual surveillance of telecommunications ordered by a targeted warrant (regarding these requirements cf. BVerfGE 141, 220 <268 *et seq*. paras. 103 *et seq*.; 309 *et seq*. para. 228 *et seq*.>).

bb) As a basis for systematically structuring the surveillance process, the legislator must set out the reasons for which strategic surveillance measures may target specific individuals. For instance, it can provide for the surveillance of individuals who might create a danger, act as messengers or as other informants. In doing so, it could draw up rules according to which the targeted surveillance of persons who are not involved in any unlawful conduct is only permissible once all other options have been exhausted. However, in this respect, too, objective thresholds for the use of powers are not required; it is sufficient that the specific purposes of targeted surveillance of individuals are determined, which, again, means that it is sufficient that measures are guided by the purposes pursued. 187

The legislator must create a separate mechanism for the protection of individuals that could be of direct interest to the Intelligence Service, either because they might create a danger or because of follow-up measures to be taken against them. Surveillance measures targeting such persons are particularly intrusive and it is especially likely that such measures will adversely affect those targeted. In the oral hearing, the Federal Intelligence Service stated that currently approximately 5% of search terms target such persons. Insofar as surveillance measures target specific persons in this manner, the determination of such measures requires *ex ante* oversight that resembles judicial review. Such oversight must assess whether the targeted surveillance of specific individuals for achieving the purpose of surveillance satisfies proportionality requirements. 188

cc) For the rest, the possibility of authorising surveillance not based on specific grounds reaches its limits where, by definition, the use of search terms targeting specific individuals – with comparable certainty – results in the targeted surveillance of individual telecommunications that is equivalent to surveillance authorised by a targeted warrant. In that case, the legislator must ensure that the requirements regarding such surveillance authorised by a targeted warrant (cf. BVerfGE 141, 220 <268 *et seq*. para. 103 *et seq*.; 309 *et seq*. para. 228 *et seq*.>) are observed and that they are not circumvented through strategic surveillance. 189

dd) The legislator may only refrain from imposing the abovementioned requirements and restrictions (see para. 187 *et seq*. above) if surveillance measures are solely aimed at providing political intelligence to the Federal Government, and if any sharing of the intelligence with other bodies is ruled out in principle (see para. 177 above). 190

f) The authorisation to carry out strategic surveillance must also be restricted by law insofar as it permits the retention of traffic data in its entirety. The legislator must en- 191

sure that the data flows intercepted to this end are substantially limited and that the data is not stored for more than six months (cf. also BVerfGE 125, 260 <322>).

g) It is sufficient that the legislator provides for the basic framework governing the specific steps for the analysis of the intercepted data and tasks the Federal Intelligence Service with creating a detailed structure for analysis in its intelligence service manual, which must be subject to independent oversight (see para. 272 *et seq*. below). This basic framework to be determined by the legislator includes the requirement that the Federal Intelligence Service analyse intercepted data without undue delay (cf. BVerfGE 100, 313 <385 and 386>; 125, 260 <332>; see also the corresponding provision in § 6(1) first sentence of the Article 10 Act and the accompanying legislative materials BTDrucks 14/5655, p. 13), the applicability of the principle of proportionality to the selection of search terms – which is already provided for in the existing intelligence service manual –, provisions governing the use of intrusive methods of data analysis, in particular complex forms of data cross-checking (regarding the particular need for safeguards applicable to the analysis of strategic surveillance cf. also ECtHR, Big Brother Watch and Others v. the United Kingdom, Judgment of 13 September 2018, no. 58170/13 and others, §§ 346 and 347), and adherence to prohibitions of discrimination under the Basic Law (regarding this requirement cf. BVerfGE 115, 320 <348>; 133, 277 <359 and 360 para. 189>; regarding the applicable law in Sweden cf. ECtHR, Centrum för Rättvisa v. Sweden, Judgment of 19 June 2018, no. 35252/08, § 29). The legislator may also have to lay down how algorithms may be used, in particular to ensure that their use can generally be reviewed by the independent oversight regime. 192

h) Confidentiality in relationships of trusts – such as relationships between journalists and their sources, or lawyers and their clients – requires special protection. Such protection already follows from Art. 10(1) GG and the proportionality requirements derived therefrom. It corresponds to a greater need for protection that may arise for any of the communicating parties involved in such relationships. For the affected professions, this protection is also guaranteed by Art. 5(1) second sentence GG or the fundamental rights that otherwise protect the respective professions – insofar as they are applicable to foreign surveillance according to their personal scope of protection. 193

The targeted surveillance of communications of professions and groups of persons whose communication relations require special confidentiality protection must be limited. The use of search terms resulting in the targeted interception of telecommunication connections belonging to such persons cannot simply be justified by the assertion that they might serve to obtain potentially relevant intelligence. It is not justified that persons doing journalistic work face a higher risk of surveillance than other fundamental rights holders and that the information which such persons gather from their contacts or research can be siphoned off for the pursuit of security interests (cf. BVerfGE 107, 299 <336>). The same applies accordingly to lawyers. The targeted surveillance of lawyers as messengers must be tied to qualified thresholds, including in the context of strategic surveillance. These thresholds must ensure that the intrusion into 194

relationships of trust is only permissible where it is used to investigate dangers that are deemed serious in the individual case and to investigate particularly serious criminal acts, or to apprehend certain dangerous criminals. This must be based on sound intelligence. For the rest, surveillance and analysis are only permissible where, in a balancing of interests conducted in the individual case, the public interest in obtaining the information takes precedence over the affected person's interest in the protection of confidentiality (cf. BVerfGE 129, 208 <258 *et seq*.>; 141, 220 <318 and 319 para. 255 *et seq*.>). The legislator will have to examine whether and to what extent it must differentiate between different kinds of relationships of trust (cf. § 160a StPO; BVerfGE 129, 208 <259 and 260>). In any case, *ex ante* oversight resembling judicial review must in principle ensure that such relationships are protected.

If it only becomes apparent during analysis that data concerning relationships of trust meriting special confidentiality protection has been intercepted, it must be assessed whether the relevant requirements are met and, if that is the case, it must then be determined in a balancing of interests whether the respective communications may be analysed and used ([…]). In this case, too, it is decisive whether the measures are expected to yield intelligence on serious and fairly specific dangers (*sich konkret abzeichnende Gefahren*) and whether the public interest in obtaining this intelligence takes precedence over the protection of confidentiality when balancing these interests against one another in the individual case. Such a decision must be subject to oversight resembling judicial review. 195

bb) For protecting professional groups and their activities abroad in the context of foreign surveillance, the legislator can take into account the different conditions under which the press or lawyers operate in other countries. Accordingly, it can limit protection to persons or situations that actually merit protection, which means that their activities are characterised by freedom and independence that justify the special fundamental rights protection afforded such institutions ([…]). What is decisive in this respect are the value decisions deriving from the fundamental rights of the Basic Law, which are integrated into international human rights guarantees (cf. Art. 1(2) GG). Uncertainties must be addressed on the basis of informed assessments. 196

cc) It is primarily for the legislator to assess whether and to what extent other relationships of trust require protection. 197

dd) Insofar as surveillance measures are exclusively aimed at providing political intelligence to the Federal Government, are not linked to any aim of early detection of dangers and the sharing of intelligence with other bodies is ruled out in principle (see para. 177 above), the legislator can refrain from protecting relationships of trust where necessary. 198

i) Art. 10(1) GG in conjunction with Art. 1(1) GG gives rise to further requirements for the protection of the core of private life. 199

aa) The protection of the core of private life guarantees the individual a domain of 200

highly personal life and ensures an inviolable core of human dignity that is beyond the reach of the state and provides fundamental rights protection against surveillance. Even exceptionally significant interests of the general public cannot justify an interference with this domain of private life that is absolutely protected (cf. BVerfGE 109, 279 <313>; 141, 220 <276 para. 120>; established case-law). This also applies to intelligence services (cf. BVerfGE 120, 274 <335 *et seq*.>) and to surveillance measures in other countries.

The free development of one's personality within the core of private life encompasses the possibility of expressing internal processes, reflections, views and experiences of a highly personal nature. Protection is afforded particularly to non-public communication with persons enjoying the highest level of personal trust, conducted with the reasonable expectation that no surveillance is taking place. Such conversations do not lose their overall personal character merely because they concern both highly personal and everyday matters (cf. BVerfGE 141, 220 <276 and 277 para. 121; 279 para. 128; 314 and 315 para. 243>; established case-law). 201

However, communications in which criminal acts are discussed and planned do not form part of the core of private life, not even when they also concern highly personal matters. This does not mean that the core of private life were subject to a general balancing against public security interests. A highly personal conversation is not excluded from the core of private life simply because it could provide insights that could be helpful for the investigation of criminal acts or the averting of dangers to public security. Statements made in the course of a conversation that only reveal inner impressions and feelings and do not contain any indications pointing to specific criminal acts do not simply become relevant to the public because they might reveal the reasons or motives for criminal conduct. Furthermore, despite having some link to criminal conduct, situations in which individuals are in fact encouraged to admit wrongdoing or to prepare for the consequences thereof, such as confessions or confidential conversations with a psychotherapist or defence lawyer, are part of the highly personal domain (cf. in this respect in more detail BVerfGE 141, 220 <276 and 277 paras. 121 and 122>; established case-law). 202

bb) The legislator must enact provisions that expressly protect the core of private life. 203

First and foremost, it must be absolutely impermissible to make the core of private life a target of state investigations and to use information relating to that core in any way or to otherwise base further investigations on it. This also applies to strategic surveillance. In line with the notion of the core of private life set out above, protection of that core must not be limited to situations which exclusively concern highly personal matters. 204

Moreover, the core of private life must be protected both at the stage of data collection and at the stage of data analysis. However, the requirements for how this protection is to be ensured by law differ based on the type of the surveillance measures in 205

question (cf. BVerfGE 141, 220 <279 para. 127>).

Accordingly, where data collection and the use of search terms for strategic surveillance measures are concerned, legislative safeguards going beyond the prohibition of the targeted collection of data from the core of private life are not required. Given that it can generally not be ascertained from the search terms as such that communications relating to the core of private life will in all likelihood be intercepted, no specific provisions are required that are aimed at removing selectors relating to the core of private life prior to data collection. This does not alter the fact that, insofar as it can be ascertained that the use of search terms will in all likelihood result in the interception of communications relating to the core of private life, such communications must, where possible, be technically excluded from interception prior to data collection (cf. BVerfGE 141, 220 <306 and 307 para. 218 *et seq*.>). 206

At the stage of manual data screening, the law must ensure that further screening ceases as soon as it becomes ascertainable that surveillance is encroaching on the core of private life; even where mere doubts arise, the measure may only be continued – subject to exemptions for cases of urgency (cf. BVerfGE 141, 220 <280 para. 129>) – in the form of recordings that are examined by an independent body prior to analysis (cf. BVerfGE 141, 220 <279 and 280 para. 129>; see also § 3a second to eleventh sentence of the Article 10 Act). It must be ensured that intelligence from the highly personal domain must not be used and must be deleted immediately; this must be documented and the deletion logs must be retained for a sufficiently long period so as to allow for oversight under data protection law (cf. BVerfGE 141, 220 <280 para. 129>; see also para. 289 *et seq*. below). 207

j) The principle of proportionality also gives rise to deletion obligations with regard to surveillance measures. The purpose of these obligations is to ensure that the use of personal data remains limited to the purposes justifying the data processing, and that data can no longer be used once these purposes have been achieved (cf. BVerfGE 65, 1 <46>; 133, 277 <366 para. 206>; 141, 220 <285 and 286 para. 144>; established case-law). 208

Surveillance measures such as those in question here, which intercept large volumes of data only part of which may be accessed for analysis, must be subject to clear provisions on deletion; these provisions must ensure that data that was unintentionally intercepted, but for which screening of its contents is impermissible under constitutional law, is immediately separated from the other data and is permanently deleted without any trace. Insofar as data analysis is carried out in several steps in which the volume of data is progressively reduced, specific provisions are required to ensure that data is swiftly analysed and that, at every stage, data identified for deletion is deleted immediately (cf. BVerfGE 100, 313 <385; 400>). Insofar as information is categorised as relevant and is to be stored for a longer period to allow for further use, corresponding provisions must be enacted. The legislator must create obligations to monitor data storage at sufficiently short intervals (cf., e.g., § 6(1) of the Arti- 209

cle 10 Act; BVerfGE 100, 313 <400>) to ensure that data is not kept without justification.

The key steps of the data deletion process must be documented, insofar as this is practical and necessary for independent oversight; the deletion logs must be retained for a sufficiently long period to allow for effective oversight (cf. BVerfGE 141, 220 <302 and 303 para. 205>; see also para. 291 below). 210

III.

Personal data stemming from strategic surveillance may only be shared with other bodies if a clear and sufficiently specific statutory basis exists that makes such sharing contingent upon the protection of legal interests and upon certain thresholds that reflect the weight of interference resulting from strategic surveillance. The sharing of personal data stemming from strategic surveillance is only permissible for the purpose of protecting legal interests of particularly great weight and requires, as a threshold, indications of an identifiable danger (*konkretisierte Gefahrenlage*) or sufficiently specific grounds for the suspicion of criminal conduct (*hinreichend konkretisierter Tatverdacht*). This does not apply to reports provided to the Federal Government, insofar as these are exclusively intended to provide political intelligence and prepare government decisions. 211

1. Where an authority makes data collected by it accessible to another body through data sharing, this amounts to a separate interference with fundamental rights (cf. BVerfGE 100, 313 <367>; 141, 220 <334 para. 305>; established case-law). This interference must be measured against the fundamental rights which the original data collection interfered with (cf. BVerfGE 100, 313 <367>; 141, 220 <334 para. 305>; established case-law). 212

2. Given that it results in new interferences with fundamental rights, data sharing requires a separate statutory basis that must be clear and sufficiently specific (cf. BVerfGE 65, 1 <46>; 100, 313 <389>; established case-law). 213

As data sharing amounts to a separate interference with fundamental rights, sharing or exchanging data stemming from particularly intrusive surveillance measures without a separate statutory basis is impermissible; such a statutory basis also serves to warn of such sharing and to clarify the applicable conditions. 214

The principle of legal clarity sets limits to the use of chains of references in legislation. A clear statutory basis is not lacking merely because a provision refers to another provision. However, such references must be limited, they must not become unclear through the referencing of provisions that concern different situations and must not result in excessive difficulties in their practical application. Obscure chains of references are therefore incompatible with the constitutional requirements (cf. BVerfGE 110, 33 <57 and 58; 61 *et seq*.>). 215

3. In substantive terms, both the statutory authorisations for data sharing and the 216

specific data sharing measures must satisfy the proportionality requirements (cf. BVerfGE 65, 1 <45 and 46>; 100, 313 <390 *et seq*.>; 141, 220 <327 para. 286>). Data sharing must be suitable and necessary for achieving a legitimate purpose. According to established case-law, the determination of whether a data sharing measure is proportionate in the strict sense must be based on the weight of the change in purpose resulting from data sharing compared to the purpose of the original data collection and, on this basis, on the criterion of a hypothetical recollection of data. According to this criterion, it is decisive whether it would be permissible under constitutional law to also collect the data in question for the changed purpose using comparably intrusive means (cf. BVerfGE 141, 220 <327 *et seq*. para. 287 *et seq*.>).

However, special circumstances must be taken into consideration for the constellation at hand. While authorities usually collect data specifically for their own operational purposes and the data is then used for a new purpose when it is shared with other authorities, the Federal Intelligence Service does not collect data for its own operational purposes, but merely with the aim to share it with the Federal Government and, as the case may be, other bodies after having identified and processed the relevant information (cf. § 1(2) BNDG). Moreover, the powers to collect data in question here are not tied to objective thresholds but are essentially only guided by the purpose pursued. 217

Especially for this constellation, adherence to substantial requirements regarding data sharing is thus of great significance. Data collection for the purpose of foreign surveillance does not require verifiable thresholds so as to allow for the identification of and proactive search for threats and situations of danger as purely precautionary measures long before specific dangers (*konkrete Gefahren*) actually arise. Under constitutional law, this requires that such thresholds must apply at least to the sharing of intelligence thus obtained ([…]). The purpose of data collection and the purpose of data sharing converge: The Federal Intelligence Service has far-reaching powers to gather intelligence to enable it to identify important information from a large volume of largely unstructured data before any operational actions are taken. A key purpose of data collection is the distinction between relevant and irrelevant data, which determines what information is provided to the government and, as the case may be, further bodies that have executive powers. However, the provisions on data sharing must then ensure that intelligence obtained on the basis of powers that are essentially not tied to specific grounds can only be used further if it were permissible, under the general requirements arising from the rule of law, to collect the data for the purposes for which the shared data is to be used . 218

Thus, whether the sharing of data is constitutional depends on whether it were permissible, under constitutional law, to collect the data for the purpose for which the shared data is to be used using comparably intrusive means (cf. BVerfGE 141, 220 <328 para. 288>). Since it is impermissible from the outset to make an instrument which is as sweeping as telecommunications surveillance that is not based on specific grounds available to domestic security authorities, the constitutional require- 219

ments that are also applicable to other particularly severe and intrusive measures such as the surveillance of private homes or remote searches apply (cf. BVerfGE 141, 220 <271 para. 110; 273 and 274 paras. 115 and 116; 327 *et seq*. para. 287 *et seq*.>), unless measures merely serve to provide reports to the Federal Government (see para. 223 *et seq*. below). This is in line with, and further determines, the requirement of an exceptionally significant public interest and of sufficiently specific and qualified thresholds for data sharing that the Federal Constitutional Court laid down in its decision on the Counter-Terrorism Database in relation to the sharing of information obtained by the intelligence services with authorities that carry out operational measures (cf. BVerfGE 133, 277 <329 para. 123>).

4. In light of the foregoing, requirements must be set both regarding the protection of legal interests and regarding thresholds for the use of powers, in this case thresholds for data sharing. These must distinguish between data sharing for public security purposes and for law enforcement purposes (cf. BVerfGE 100, 313 <394>; 141, 220 <270 and 271 paras. 107 and 108>). 220

In terms of the protection of legal interests, data sharing for public security purposes is only permissible to protect particularly weighty legal interests (cf. BVerfGE 125, 260 <329 and 330>; 133, 277 <365 para. 203>; 141, 220 <270 para. 108>). Insofar as the law provides for a change in purpose, data sharing does not have to serve the protection of the same legal interest as the warrant authorising surveillance by the intelligence service. In principle, such sharing must be directly based on a legal interest, rather than on statutory catalogues of criminal offences; in any case, a reference to criminal offences must not include the criminalisation of preparatory acts or mere threats to legal interests, which would shift the threshold at which acts become punishable to a time before a danger actually arises (cf. BVerfGE 125, 260 <329 and 330>). By contrast, data sharing for law enforcement purposes must be limited to criminal offences of great weight. Based on these criteria, such sharing is only justified if it serves to prosecute particularly serious criminal offences. These particularly serious criminal offences must generally be determined in statutory catalogues. 221

In terms of thresholds for data sharing, sufficiently specific indications that a danger may emerge (*hinreichend konkret absehbare Gefahrenlage*) are required to justify data sharing for public security purposes. The legislator does not have to make data sharing contingent upon the existence of a specific (*konkrete Gefahr*), immediate (*unmittelbar bevorstehende Gefahr*) or present danger (*gegenwärtige Gefahr*) as is traditionally required for public security measures. However, the statutory basis must require an identifiable danger in the sense that there be at least factual indications that a specific danger to the protected legal interests may emerge (cf. in this respect BVerfGE 141, 220 <271 *et seq*. para. 111 *et seq*.>). Insofar as data is shared for law enforcement purposes, there must be sufficiently specific facts that give rise to the suspicion that a particularly serious criminal act has been committed. Mere indications that are sufficient to launch initial, general investigations (cf. § 152(2) StPO) do not suffice here; rather, specific facts are required that give rise to the suspicion that 222

such criminal acts have been committed (cf. BVerfGE 125, 260 <328 and 329>), which corresponds to the requirements for the surveillance of private homes pursuant to § 100c StPO. In this respect, there must be circumstances that have taken specific shape to some extent and support such a suspicion ([…]).

5. This does not apply to the sharing of intelligence stemming from strategic surveillance with the Federal Government solely in its governmental capacity. Where information is provided to the Federal Government so that it can discharge its responsibility with regard to foreign and security policy and a transfer to other bodies is ruled out, qualified protection of legal interests or thresholds for data sharing are not required under constitutional law. 223

a) Such further requirements are not needed here given that providing information to the Federal Government on matters that are significant to foreign and security policy is the primary purpose of foreign surveillance and the provision of such information constitutes an exceptionally significant public interest even if there are no indications that a specific danger may emerge. 224

Most notably, where surveillance is only used to provide political intelligence to the Federal Government, its weight of interference vis-à-vis the person under surveillance is generally significantly lower. Insofar as such intelligence does not concern government officials of other states, in respect of which surveillance can in principle be justified by public interest, personal data will often be irrelevant to such reports provided to the Federal Government so that it can, or even must, be deleted. But even where it is necessary to include personal data in such reports, these reports differ fundamentally from the sharing of intelligence concerning individuals with domestic authorites that – directly or indirectly – have executive powers and may use these powers against those individuals. This is all the more true when comparing such reports to the sharing of intelligence with foreign bodies. When intelligence is used as background information for the Federal Government or as a basis for preparing governmental decision-making, the interest in the individuals concerned typically becomes less important; therefore, sharing can be justified regardless of whether specific thresholds for data sharing are observed. 225

However, such reports to the Federal Government solely serve to provide political intelligence at the governmental level. Insofar as this intelligence is provided irrespective of the adherence to thresholds for data sharing, its use is therefore limited to decisions made by the Federal Government itself regarding foreign and security policy. The Federal Government can use this intelligence to perform its duties – including communicating with foreign governments and international organisations – as long as it does not share it with domestic or foreign subordinate agencies for other, in particular operational, purposes. The same applies to the Federal Government's interaction with *Land* governments. 226

b) Insofar as intelligence stems from surveillance measures carried out for the purpose of early detection of dangers and thus serves both the provision of intelligence 227

to the Federal Government and the early detection of dangers – which appears to be common practice –, such intelligence may be used for purposes other than government activities. However, where such intelligence is intended to be shared with bodies other than the Federal Government or *Land* governments that carry out operational work – in particular security authorities or domestic administrative authorities – statutory authorisations for sharing the data are required, as is the case for the direct sharing of data with other bodies. These authorisations must satisfy the above-mentioned requirements regarding qualified protection of legal interests and the existence of thresholds.

c) Yet even if provisions on data sharing do exist, data sharing with other bodies must generally be ruled out if data stems from surveillance measures which were not, from the outset justified by the aim of early detection of dangers and were carried out merely to provide political intelligence to the Federal Government irrespective of any surveillance interest relating to dangers (see paras. 177 and 226 above). In such cases, intelligence must not be shared with other bodies, including by means of a regular change in purpose. The legislator may only provide for an exemption insofar as the data indicates, in and of itself, an immediate danger to life, limb or liberty of the person, vital interests of the public or the existence or security of the Federation or a *Land* (see para. 174 above). 228

6. Given that the sharing of data with other bodies amounts to a separate interference with fundamental rights, it requires a formal decision by the Federal Intelligence Service – just as other agencies must make a formal decision when they share personal data with the Federal Intelligence Service – as part of which it must be ensured that the respective statutory requirements for data sharing are satisfied. Given its broad powers, the Federal Intelligence Service has a special responsibility in this respect. On the one hand, its powers are especially broad, allowing for the interception of personal data that is not based on specific grounds for the early detection of dangers; on the other hand, it must thoroughly screen the intelligence obtained before sharing it and must limit it to what is necessary in accordance with the respective provisions on data sharing. Insofar as it is not reports made only to the Federal Chancellery or individual Federal Ministers and the use of these reports by the Federal Government that are concerned, data sharing must be documented so as to ensure independent oversight of adherence to the requirements for data sharing (cf. BVerfGE 141, 220 <340 and 341 para. 322>; see also para. 291 below). Such documentation must also specify the statutory provision on which data sharing is based. 229

This does not affect the possibility of combining information held by different bodies and of facilitating the sharing of such information through joint databases, such as the one provided for by the Counter-Terrorism Database Act (regarding the constitutional requirements arising from this BVerfGE 133, 277 <320 *et seq*. para. 105 *et seq*.>). 230

7. Special requirements apply to the sharing of data with foreign bodies. First of all, 231

this concerns intelligence sharing in the individual case – irrespective of whether this occurs within the context of cooperation (regarding automated data sharing in the context of cooperation see paras. 254 *et seq*. and 262 *et seq*. below).

a) The requirements set out above regarding the protection of legal interests and thresholds for sharing data with domestic bodies apply to the sharing of data with foreign bodies, too (see paras. 216 *et seq*. and 220 *et seq*. above). While these requirements do not prevent the legislator from accommodating the autonomy of foreign legal orders in the wording of the authorisations, the substantive level of protection is not called into question (cf. BVerfGE 141, 220 <343 para. 331>). 232

b) In addition, however, a separate requirement when sharing data with foreign bodies is the ascertainment that the foreign bodies will handle the data shared with them in accordance with the rule of law. This reflects the fact that, once shared with foreign bodies, the use of data collected by German authorities is no longer subject to the requirements of the Basic Law since the foreign state authority is only bound by its own laws, yet German state authority is responsible for the sharing of data and is bound by the fundamental rights when sharing data (cf. BVerfGE 141, 220 <342 paras. 326 and 327>). 233

According to established case-law, the state receiving the data is required to adhere to guarantees under data protection law (see aa) below) and to uphold human rights when using the information (see bb) below). Both require clear provisions ensuring that the Federal Intelligence Service sufficiently ascertain that these guarantees will be upheld (see cc) below). In addition, adherence to restrictions on the sharing of data collected through strategic surveillance must be ensured by obtaining sound assurances from the receiving states (see dd) below). 234

aa) The first requirement serves to uphold the data protection guarantees following from the right of personality. Yet it is not required that receiving states have rules on the processing of personal data that match those within the German legal order or that they guarantee protection that is equivalent to the protection afforded by the Basic Law. In fact, the Basic Law recognises the autonomy and diversity of legal orders and it generally respects them, including in the context of data sharing. Value decisions and parameters [in receiving states] do not have to conform to those of the German legal order or the Basic Law. 235

However, the sharing of personal data with other states is only permissible if the handling of the shared data in these states does not undermine the protection of personal data guaranteed by human rights. This is not to say that the other state's legal order must guarantee institutional and procedural safeguards corresponding to Germany's; in particular, it is not necessary that there be the same formal and institutional safeguards as required under data protection laws applicable to German bodies. What is required is the guarantee of an appropriate substantive level of data protection for the handling of the shared data in the receiving state. In this respect, it must be considered in particular whether limits resulting from purpose limitation, deletion 236

requirements as well as fundamental requirements for oversight and data security – all of which were communicated in the course of data sharing – are at least generally observed in data usage. The assessment of whether this is the case must be made on the basis of the receiving state's domestic law as well as its international obligations and the implementation thereof in everyday practice (BVerfGE 141, 220 <344 and 345 paras. 334 and 335> with further references).

bb) Sharing data with other countries is ruled out if there is reason to fear that its use would lead to violations of fundamental principles of the rule of law. Under no circumstances may the state be complicit in violations of human dignity (cf. BVerfGE 140, 317 <347 para. 62>; 141, 220 <342 para. 328>). In particular, it must appear certain that the information will be used neither for political persecution nor for inhuman and degrading punishment or treatment in the receiving state (cf. Art. 16a(3) GG). The legislator must ensure that the sharing of data collected by German authorities with other countries or international organisations does not erode the protections of the European Convention on Human Rights and other international human rights treaties (cf. Art. 1(2) GG; cf. BVerfGE 141, 220 <345 para. 336>). Given the exceptional nature of surveillance and data sharing measures carried out by intelligence services, which may involve contacts with states not firmly committed to the rule of law, it must be ensured that the information provided is not used to persecute certain ethnic groups, stifle opposition or detain people without due process, kill or torture them in violation of human rights or international humanitarian law. The Federal Intelligence Service itself is responsible for examining and determining which rules of international law have to be observed in this respect. In principle, receiving states must agree to rights to information so that adherence to international human rights standards can be monitored. 237

cc) To uphold this standard of protection, clear statutory provisions are required that impose an obligation on the Federal Intelligence Service to ascertain the necessary level of protection abroad. Before sharing data, the Federal Intelligence Service must ascertain that the receiving state adheres to requirements arising from data protection law and from human rights. 238

(1) This ascertainment does not require a comprehensive assessment in the individual case or binding individual assurances in every respect, but can be based on a generalised assessment of the factual and legal situation in the receiving states. Yet the assessment must be designed in such a way that adverse facts are taken into account and it must be refutable (cf. BVerfGE 140, 317 <349 para. 69>). Where such generalised assessments are not tenable, a fact-based assessment in the individual case is necessary; such an assessment must conclude that adherence to at least essential requirements for the handling of data is sufficiently guaranteed. Where necessary, binding individual guarantees can and must be provided. In principle, binding assurances are a suitable means for overcoming concerns regarding the permissibility of data sharing, as long as it is not to be expected that the assurances will not be adhered to in the individual case (cf. BVerfGE 63, 215 <224>; 109, 38 <62>; 140, 239

317 <350 para. 70>). The legislator may also choose to determine which requirements apply in a specific constellation on the basis of a balancing of interests in the individual case (BVerfGE 141, 220 <345 and 346 paras. 337 and 338>).

The Federal Intelligence Service must be particularly prudent given that in the context of strategic surveillance, data is largely collected irrespective of whether affected persons are, from an objective perspective, involved in a situation of danger and given that some of the data relates to circumstances in states not firmly committed to the rule of law and concerns highly political, tense situations. Even insofar as assessments regarding certain states may be generalised in principle, an assessment of possible risks in the specific case is always required if there is any indication that data sharing could put affected individuals in jeopardy. To the extent that the shared data includes data of journalists, lawyers or other professions meriting confidentiality protection, including to shield them from risks, a separate balancing of interests is required that differs from the balancing conducted to determine whether such data may be used domestically (see para. 193 *et seq*. above); it must generally be subject to *ex ante* oversight resembling judicial review (cf. United Nations Office of the High Commissioner for Human Rights, Letter of the Special Rapporteurs of 29 August 2016, OL DEU 2/2016, p. 7). 240

(2) The ascertainment that the required level of protection is adhered to is not a decision that is at the free discretion of politicians. It must be based on substantive, reality-based and up-to-date information. It must be documented and must be accessible to independent oversight (cf. BVerfGE 141, 220 <346 para. 339>). Especially weighty instances of data sharing or those in respect of which it is difficult to assess which legal requirements apply may necessitate further procedural safeguards, such as prior authorisation by the head of the intelligence service or the head of the Federal Chancellery or – as in the case of the sharing of information concerning journalists or lawyers meriting protection – *ex ante* oversight resembling judicial review. 241

dd) Given that the data collected by the Federal Intelligence Service in the context of strategic telecommunications surveillance stems from surveillance measures not based on specific grounds, it is especially important that effective limits are observed regarding the sharing of such intelligence with authorities that have operational powers, in particular law enforcement and police authorities or domestic administrative authorities. Insofar as the Federal Intelligence Service shares intelligence with foreign intelligence services, an obligation must be imposed on it – in line with current practice – to generally make such sharing contingent upon the assurance that the foreign service will only share the intelligence with other bodies if the Federal Intelligence Service consents. As the case may be, it may also be sufficient that the foreign service assures the Federal Intelligence Service that it will only share intelligence on specific persons with other bodies if there is reliable information suggesting that the persons on whom intelligence is shared are responsible for, or involved in, a specific and particularly serious danger based on objective circumstances or – insofar as sharing with intelligence services in third states is concerned – that sharing is made 242

conditional upon a corresponding assurance (regarding assurances in the context of cooperation see paras. 259 *et seq*. and 264 below). This requires, as it does for all such assurances, that it can be assumed that the intelligence service in question will keep their assurances and that, in addition, the Federal Intelligence Service is granted rights to information vis-à-vis the foreign service.

IV.

The design of a statutory basis for the cooperation with foreign intelligence services in the context of strategic telecommunications surveillance gives rise to special constitutional challenges. In the context of such cooperation, the legislator intends to enable the Federal Intelligence Service to analyse the intercepted data traffic by means of search terms determined by other intelligence services and to share the resulting matches with them in an automated manner; in addition, traffic data is to be shared with partner services without undergoing prior analysis. In return, the Federal Intelligence Service should be allowed to use the data and capacities of other services. This mutual exchange serves to broaden the data available for the use of search terms and to use existing capacities more effectively (cf. BTDrucks 18/9041, p. 29). 243

Such legal provisions can only satisfy the requirements arising from fundamental rights if it is ensured that the limits to strategic surveillance set by the rule of law are not set aside through the mutual sharing of intelligence and that the Federal Intelligence Service essentially remains responsible for the data it has collected and analysed ([…]). 244

1. As a constitutional order that is open to international law, the Basic Law permits such cooperation with foreign intelligence services. However, it requires separate statutory provisions ensuring that fundamental rights protection is also guaranteed in the context of international cooperation between intelligence services. 245

a) With its Preamble, together with Art. 1(2), Art. 9(2), Art. 16(2), Arts. 23 to 26 and Art. 59(2) GG, the Basic Law comprehensively binds the Federal Republic of Germany to the international community and has programmatically aligned German state authority towards international cooperation (cf. BVerfGE 141, 220 <341 and 342 para. 325> with further references). This also applies to ensuring public security. The Federal Constitutional Court has highlighted that effective cooperation with the security authorities of other states can be especially significant for public security. In the interest of the constitutionally mandated protection of individuals, effective information sharing can require the transfer of intelligence gathered domestically and in return rely on intelligence provided by foreign bodies (cf. BVerfGE 141, 220 <268 para. 102>). 246

Accordingly, the Basic Law is open to cooperation of the Federal Intelligence Service with other intelligence services. Such international cooperation can be essential for protecting Germany’s foreign and security policy interests and, in this context, for maintaining public security; it can be based on the Basic Law’s openness to interna- 247

tional cooperation (cf. also BVerfGE 143, 101 <152 *et seq*. para. 168 *et seq*.>). Thus, the Federal Intelligence Service may be granted the authorisation to use its powers for the intelligence interests of foreign services and states. These interests must be comparable to legitimate intelligence interests of the Federal Intelligence Service and compatible with Germany's foreign and security policy interests. Moreover, the shared data must be used in accordance with the rule of law.

b) However, cooperation in the field of telecommunications surveillance must be designed in such a way that fundamental rights protection against covert surveillance measures and the resulting requirements regarding data collection, processing and sharing are not circumvented. This applies in particular to the protection against domestic surveillance, which must not be compromised through the free sharing of intelligence stemming from surveillance measures by foreign intelligence services that target Germany. Such sharing in a circle (*Ringtausch*) is not permissible under constitutional law. This applies accordingly with regard to the fundamental rights requirements that the Federal Intelligence Service must satisfy when conducting surveillance of foreign telecommunications. 248

Foreign intelligence services themselves may only be granted the power to carry out surveillance measures from within Germany and such measures may only be tolerated if there are specific grounds for carrying out the measures and if detailed statutory provisions ensure that fundamental rights apply without any reservations, both in substantive and in procedural terms. The protection afforded by fundamental rights entails a duty of the German state to protect individuals under Germany's jurisdiction against surveillance measures conducted by other states in a manner that violates fundamental rights ([…]). Cooperation cannot exempt the German state from this duty. 249

c) In addition, the cooperation with foreign intelligence services requires a separate statutory basis. Firstly, legal provisions are necessary to the extent that the Federal Intelligence Service wants to gain access to surveillance open to foreign intelligence services, and wants to obtain and use the data collected by them. These provisions must cover both the sharing of search terms by the Federal Intelligence Service with a foreign intelligence service for use and analysis by that service and the retrieval or receipt of data made available by a foreign partner for analysis by the Federal Intelligence Service by means of selectors or other techniques (regarding the necessity of such rules cf. also ECtHR, Big Brother Watch and Others v. the United Kingdom, Judgment of 13 September 2018, no. 58170/13 and others, § 424). Such provisions must reflect the possibility inherent in such practices that obligations under domestic law could be circumvented (cf. also ECtHR, *loc. cit*.) and the specific risks to fundamental rights which may arise from cooperation. In this respect, the law must set out to what extent the Federal Intelligence Service can, in the context of cooperation, receive and use intelligence on specific individuals from foreign services in respect of which there is an indication that it was obtained through the surveillance of German domestic communications. Since the legislator has not enacted such provisions yet, 250

the present proceedings are not concerned with the requirements applicable to such provisions.

Secondly, legal provisions are required to the extent that the Federal Intelligence Service is to be granted powers for surveillance and data sharing that it can also use in the interest and under the guidance of other intelligence services. If the legislator wants to allow the Federal Intelligence Service to analyse the data collected by it by means of search terms provided by its foreign partners or to automatically share pre-filtered content data or, as the case may be, even unfiltered traffic data with foreign services, it must create a separate statutory basis for this, as it essentially did when enacting §§ 14 and 15 BNDG. 251

2. The constitutional requirements applicable to such a statutory basis are designed to ensure that the general limits to strategic surveillance arising from fundamental rights are upheld as effectively as possible in the context of cooperation. 252

Given that such cooperation can only take place if the strict protection of domestic communications is guaranteed, it must be limited to data obtained through the surveillance of foreign telecommunications (see para. 170 *et seq*. above). Thus, with regard to data collection and analysis by the Federal Intelligence Service in the context of cooperation, it must be ensured that, where possible, telecommunications data of persons within Germany and German citizens is not shared, or, if it is only identified at a later stage, is immediately deleted, so as to uphold the protection guaranteed by Art. 10(1) GG. This also means that both the search terms provided by foreign partners and the data that is designated for automated sharing with foreign partners must be filtered (for more detail see paras. 255 *et seq*. and 264 below). The requirements set out above (see para. 170 *et seq*.) also apply in this case. Moreover, for the cooperation between intelligence services, too, the legislator must determine, in a sufficiently precise and clear manner, the purposes for which surveillance conducted through the interaction of intelligence services is permissible, and must limit them to the protection of high-ranking interests of the common good (see paras. 175 and 176 above). Likewise, cooperation on the basis of a formal determination of precisely defined surveillance measures must be categorised by aim, object and duration and structured by procedural safeguards (see para. 178 *et seq*. above). This does not rule out that such joint, yet delimited surveillance measures can be part of longer-term cooperation on a broader scale, which may be based on a framework agreement. Like the sharing of individual pieces of intelligence, the automated sharing of data requires an ascertainment that the shared data is used in accordance with the rule of law, which must be documented (see para. 233 *et seq*. above). This ascertainment must be obtained for each of the joint surveillance measures respectively; insofar as this becomes necessary in the course of cooperation, it must be reaffirmed (regarding the necessity of assurances, which are of special significance in the context of cooperation, see paras. 259 *et seq*. and 264 below). 253

3. Specific requirements apply insofar as, in the context of cooperation, the Federal 254

Intelligence Service wants to use search terms determined by a foreign intelligence service and then automatically share the resulting matches with the foreign partner without first conducting a content-based analysis. The legislator must create rules for this situation that ensure the Federal Intelligence Service's responsibility with regard to fundamental rights for the data collected by it and its processing.

a) First of all, this requires a thorough assessment of the search terms determined by the foreign partner and the resulting matches. The Federal Intelligence Service must assess whether the use of the search terms as such and the data selected through their use is subject to limits arising from fundamental rights. 255

aa) With regard to the search terms determined by foreign partners, this requires an assessment – in line with current practice – of whether these serve the purposes of the respective surveillance measures. The foreign intelligence services must sufficiently demonstrate why they want to use specific search terms. In addition, both the search terms and the resulting matches must be checked, for instance against lists of persons in danger; such checks aim to identify, where possible, data concerning persons or situations in respect of which there is an indication that they merit special protection, such as dissidents at risk of persecution or whistle-blowers. The existing framework provides for safeguards with regard to national interests or objectives of the European Union; likewise, special safeguards are required with regard to fundamental rights. 256

This also applies to persons whose work requires special confidentiality protection under constitutional law, in particular lawyers and journalists meriting protection. However, surveillance measures vis-à-vis these professions are not entirely ruled out even in the context of cooperation. Yet in this context as well, they can only be permissible subject to a qualified protection of legal interests, thresholds and a balancing of interests (see para. 194 *et seq*. above). In order to ensure that these requirements are met, search terms that serve to intercept telecommunications of such persons must be identified through filtering where possible, and must then undergo manual screening that includes the required balancing. To determine whether the requirements for the use of such selectors are met, the foreign partner must, where necessary, plausibly demonstrate why it wants to use them. Accordingly, prior to any automated sharing with a foreign intelligence service, the Federal Intelligence Service must check the data identified by the search terms to determine whether it can be attributed to persons whose communications require special confidentiality protection, including to prevent government crackdowns, and must, where necessary, manually screen this data. Insofar as decisions are made in the individual case in this regard, they must be subjected to oversight resembling judicial review. 257

bb) The assessment of search terms must be as effective as possible. In line with current practice, an automated assessment can initially be considered. The Federal Intelligence Service must be required by law to gather possible indications that certain persons merit or need special protection, using the intelligence and experience 258

obtained in the course of its work, and combine telecommunications identifiers relating to these persons in such a manner that it can filter search terms and data designated for sharing. The same applies accordingly to the identifiers of journalists, lawyers or similar persons, groups or organisations whose communications are afforded special confidentiality protection. The databases and filtering processes used to this end must be continually updated and developed further. Where necessary, these automated processes must be complemented by manual screening based on sufficiently comprehensive random samples. Based on information provided in the oral hearing, this must be considered indispensable, at least given the current level of effectiveness of these automated processes.

b) Obtaining substantial assurances by the partner services is particularly significant with regard to the automated sharing of data that has not been fully analysed. Given that responsibility for the analysis of data collected by the Federal Intelligence Service is placed into the hands of a foreign intelligence service, which is not bound by the Basic Law, specific assurances by this foreign service regarding the further handling of data must be obtained. Given the applicability of fundamental rights abroad, these assurances must be in line with the fundamental rights protection afforded the person under surveillance. 259

Thus, partner services must provide an assurance, firstly, that they will immediately delete data that involves German citizens or persons within Germany, insofar as they identify such data during their analysis. Secondly, they must provide substantial assurances regarding their handling of relationships of trust meriting confidentiality protection. Thirdly, assurances must be obtained to ensure that partner services will not undermine the restrictions on data sharing that are applicable to the Federal Intelligence Service (see para. 242 above). 260

Like the general ascertainment that data will be used in accordance with the rule of law, these assurances must refer to the individually determined surveillance measure and must be reiterated if a measure is renewed. They do not have to be made in a form that is binding under international law, but they must be effective in practice. The Federal Government must assess to what extent such agreements can be complemented by rights to information or notification requirements and rules on communication and intervention – such as deletion requests –, which the Federal Intelligence Service can and must use where applicable. 261

4. Finally, a separate statutory basis is required insofar as an entire set of traffic data is to be shared with foreign intelligence services in the context of cooperation, without prior selection based on specific search terms, allowing the foreign services to retain this traffic data and to analyse it using their own methods. 262

a) In this scenario, the Federal Intelligence Service hands over the data collected by it without the possibility to exercise any control over content. Therefore, such cooperation must be subject to specific restrictions. The sharing of an entire set of traffic data cannot be authorised continually and merely on the basis of the purpose pur- 263

sued, but requires a qualified need for intelligence relating to specific indications of an identifiable danger. Certain events beyond the existence of potential dangers must provide grounds for conducting surveillance measures that counter specific threats and ensure that the Federal Republic of Germany retain its capacity to act. This may be the case, for instance, where factual indications suggest that terrorist attacks are being prepared, military weapons are being moved on a certain route or coordinated cyber attacks against certain states or organisations are imminent. This must be documented when the measure is formally determined (see para. 179 *et seq*. above), and the analysis by the foreign service must be limited to this aim. The determination of such measures must be accessible to oversight resembling judicial review.

b) Moreover, in line with the general requirements (see para. 170 *et seq*. above), data relating to German citizens and persons within Germany must be separated from traffic data. Furthermore, the telecommunications data of persons in relation to whom the Federal Intelligence Service knows that they merit or require special protection must also be separated from the other data (see paras. 257 and 258 above). The requirements for ascertaining that data will be used in accordance with the rule of law remain unaffected (see para. 233 *et seq*. above). In this context, foreign services must also provide an assurance that the shared traffic data will not be retained for more than six months. The Federal Government must assess whether additional assurances can be obtained that could further ensure that the limits to surveillance and data use arising from fundamental rights are adhered to in the context of cooperation. 264

V.

In relation to surveillance measures, the principle of proportionality also gives rise to requirements regarding transparency, individual legal protection and oversight (cf. BVerfGE 141, 220 <282 *et seq*. para. 134 *et seq*.> with further references; established case-law). However, the requirements regarding transparency and individual legal protection are significantly less strict for the surveillance of foreign telecommunications. To compensate for this, the principle of proportionality gives rise to special requirements regarding independent oversight (cf. BVerfGE 133, 277 <369 para. 214>; 141, 220 <284 and 285 paras. 140 and 141>). 265

1. The requirements regarding transparency of data processing call for rights to information. In principle, this is also the case where intelligence services are concerned (cf. BVerfGE 125, 260 <331 and 332>). However, such rights to information can be restricted to the extent necessary to ensure the effective performance of the intelligence services' tasks (cf. BVerfGE 133, 277 <367 and 368 para. 209 *et seq*.>; 141, 220 <283 para. 137>). Given that surveillance of foreign telecommunications is largely carried out covertly, the rights to information of affected persons can be significantly restricted. In particular, intelligence services can be exempted from the obligation to provide specific information on how data was obtained. Thus, rights to information can only provide a basis for transparency and individual legal protection to a limited 266

extent; this must be compensated by creating a comprehensive independent oversight regime (cf. BVerfGE 133, 277 <369 para. 214>; for more detail see para. 272 *et seq*. below).

2. In principle, notification requirements are a prerequisite for the proportionate design of covert surveillance measures, regardless of whether they are carried out by intelligence services or by other security authorities. In this respect, too, the legislator may provide for exemptions, which must be balanced against the constitutionally protected legal interests of third parties and must serve to ensure the effective performance of the intelligence service's tasks. Even though such exemptions must be limited to what is absolutely necessary (cf. BVerfGE 109, 279 <364>; 125, 260 <336>; 141, 220 <283 para. 136>), the notification requirements regarding strategic surveillance are not comprehensive. 267

a) In relation to strategic surveillance concerning persons within Germany, differentiated legal provisions are required that ensure that these persons are notified wherever possible. This is particularly important where, despite the existing filtering mechanisms, communications in which Germans or persons within Germany were involved are not technically separated from other data, but are only identified during manual screening and not immediately deleted. 268

In relation to persons who are abroad, the legislator may, in principle, refrain from imposing notification requirements for strategic surveillance measures (cf. Marxsen, Die Öffentliche Verwaltung – DÖV 2018, p. 218 <227>; Dietrich, in: Schenke/Graulich/Ruthig [eds.], Sicherheitsrecht des Bundes, 2nd ed. 2019, § 6 BNDG para. 10). There is a fundamental interest in ensuring that measures carried out by the Federal Intelligence Service that have a direct impact on other countries or are carried out in those countries go unnoticed so as to ensure that the Federal Intelligence Service can perform its tasks in the long term. Any formal and specific disclosure of the fact that the Federal Intelligence Service is conducting surveillance in another state or of the possibilities for doing so can jeopardise its sources (cf. Gusy, in: Schenke/Graulich/Ruthig [eds.], Sicherheitsrecht des Bundes, 2nd ed. 2019, BNDG preliminary remarks para. 10). Notification requirements vis-à-vis persons living abroad can only serve their purpose to a very limited extent. Compared to notification provided to persons living in Germany, notification provided to persons living abroad can neither provide a basis for legal protection that is attainable in practice (cf. BVerfGE 65, 1 <70>; 109, 279 <363 and 364; 367>; 120, 351 <361>; established case-law), nor can it achieve the aim of creating public trust or of generating democratic discourse on such measures (cf. BVerfGE 125, 260 <335 and 336>; 133, 277 <366 para. 206>; 141, 220 <282 and 283 paras. 135 and 136>; established case-law). Instead, notifying affected persons in another legal order may even be dangerous, as it may expose those persons to the attention and mistrust of the authorities in their state and, as the case may be, third parties. 269

Thus, the requirements for transparency of state action are significantly less strict 270

and there are fewer possibilities for obtaining individual legal protection in practice. Recourse to the courts pursuant to §§ 40, 50(1) no. 4 of the Code of Administrative Court Procedure (*Verwaltungsgerichtsordnung* – VwGO) remains formally unaffected, yet affected persons will only be able to obtain legal protection through this avenue in exceptional cases, given that they are not aware of the surveillance measures. In this respect, too, comprehensive independent oversight is required as compensation and in order to uphold the principle of proportionality (see para. 272 *et seq*. below).

b) Where the law does not provide for notification requirements, Art. 10(2) second sentence GG may have to be observed. However, this provision does not give rise to strict constitutional requirements regarding the structure of the oversight regime that must be created to compensate [for the absence of notification requirements]. Its scope of application is narrowly restricted by its elements of "the protection of the free democratic basic order" and "the existence or security of the Federation or of a *Land*" (cf. BVerfGE 100, 313 <397 and 398>). Even where the requirements of Art. 10(2) second sentence GG are met, no detailed instructions for the structure of oversight follow from its reference to agencies and auxiliary agencies appointed by the legislature. It only lays down that the oversight body exercising review must be created by Parliament, which must also determine its members – in consideration of the different political groups represented in Parliament. The oversight body can be either a parliamentary body or a body not connected to Parliament (cf. BVerfGE 30, 1 <23>; 143, 1 <12 para. 39>). Thus, the body does not necessarily have to be made up of members of the *Bundestag*. Nor does the provision preclude organisational independence of the body, including strict confidentiality vis-à-vis Parliament as well (regarding accountability of the Federal Intelligence Service to Parliament, which follows separate principles and is not at issue in the present proceedings, cf. BVerfGE 143, 101 <133 *et seq*. para. 106 *et seq*.>). The body can also be an independent institution within the executive branch (cf. BVerfGE 30, 1 <28>; 143, 1 <12 para. 39>; see para. 274 *et seq*. below for more detail on the requirements and possibilities for the design of such a body). 271

3. Strategic telecommunications surveillance is only compatible with the proportionality requirements if it is complemented by comprehensive independent oversight that serves to ensure that the law is observed. This concerns, on the one hand, strategic surveillance and the related data use, as well as, on the other, the sharing of intelligence thus obtained and the cooperation with foreign intelligence services. Such oversight must be designed as continual legal oversight that allows for comprehensive access to conduct oversight of the surveillance process. It must be aimed at upholding the fundamental rights of affected persons. Moreover, it must serve to guarantee adherence to the legal limits of state surveillance measures and to ensure the practical effectiveness of these limits. 272

a) In relation to strategic surveillance, the constitutional requirements regarding the design of the oversight regime are particularly strict and detailed. This is because 273

oversight must compensate for the virtual absence of safeguards commonly guaranteed under the rule of law. Oversight thus serves two functions. Firstly, it must compensate for the gap in legal protection that follows from the weak possibilities for individual legal protection in practice. Given that very limited information and notification requirements apply to the surveillance of foreign telecommunications in light of its need for secrecy, effective legal protection can hardly be obtained; this must be compensated by oversight exercised by an independent body. Secondly, to compensate for the fact that surveillance powers are essentially only guided by the purpose pursued, oversight must ensure that the use of these powers adheres to the required procedure. Oversight thus serves as a counterweight to the wide-ranging possibilities for conducting surveillance that are granted to the Federal Intelligence Service and ensures, in procedural terms, that these are adequately based on the statutory aims.

b) The legislator must provide for two different types of oversight, which must also be reflected in the organisational framework. 274

aa) Firstly, a body resembling a court must be tasked with conducting oversight. This body must consist of panels with members who must be independent in a way that is equivalent to judicial independence. They must decide in a formal procedure and their decisions must be made in writing and are final and binding on the Federal Government and the Federal Intelligence Service. This type of oversight must provide the protection otherwise afforded through the requirement of prior judicial authorisation or through avenues for *ex post* legal protection, in particular declaratory actions. Thus, it must allow for a review in the individual case which is equivalent to judicial review both in substantive and in procedural terms and is at least as effective, too (cf. BVerfGE 30, 1 <23> on Art. 10(2) second sentence GG). 275

bb) Secondly, independent oversight must also be exercised by a body that is administrative in nature. In this respect, an oversight body must be created that can, on its own initiative, randomly scrutinise the entire process of strategic surveillance as to its lawfulness; this concerns individual decisions, processes, the design of data processing and filtering mechanisms as well as the technical resources used for them. This oversight body does not have to be vested with final decision-making powers; it is sufficient that the body be granted a right to object. To clarify fundamental questions of law, the body must have the option to refer such questions to the decision-making body that resembles a court (see para. 298 below regarding the necessary option to raise concerns with Parliament or the public under certain circumstances). 276

c) It is incumbent upon the legislator to set out how the competences of the different types of oversight interact. It has considerable latitude in this area, but must adhere to the requirements arising from the principle of proportionality. 277

aa) The legislator must ensure that the key procedural steps of strategic surveillance and of data processing measures linked to it are, in principle, subject to oversight that resembles judicial review and is given the power to make final decisions. In particular, as can be inferred from the substantive requirements set out above, such 278

oversight must examine the formal determination of the various surveillance measures, including in the area of cooperation; specific bulk warrants; the use of search terms, insofar as these directly target individuals who may pose a danger and are thus of direct interest to the Federal Intelligence Service; the use of search terms that directly target individuals whose communications enjoy special confidentiality protection; the balancing decisions required to protect confidentiality in relationships of trust; the handling of data that may belong to the core of private life; data sharing that requires special oversight, particularly with foreign bodies; and the requirements for cooperation that is aimed at the automated sharing of traffic data with foreign intelligence services for retention and analysis. Furthermore, oversight resembling judicial review is required with regard to the exceptional use of data based on particular situations of danger, even though this data stems from telecommunications in which Germans or persons within Germany were involved (insofar as this was only noticed during manual screening), or the data stems from surveillance measures not based on the purpose of early detection of dangers, but only on the purpose of providing political intelligence to the Federal Government. The legislator has latitude to determine whether such oversight is to be exercised *ex ante* or *ex post* and whether only random samples are screened – possibly in interaction with the administrative oversight body – in the case of *ex post* oversight. Nevertheless, the legislator is bound by the principle of proportionality – as, in part, becomes clear from the further requirements set out above –, which requires *ex ante* oversight at least for fundamental decisions.

bb) It must be guaranteed that the entire process of strategic surveillance, including the processing and sharing of data based on it and the cooperation with foreign intelligence services, can comprehensively be subjected to oversight when the oversight bodies interact. In cases in relation to which no oversight resembling judicial review is provided for, administrative oversight must be possible. Yet only oversight as to the objective legality of the measures in question is required. It does not concern a decision on whether, within the legal framework, the powers are exercised adequately in practice. 279

cc) With regard to oversight resembling judicial review, the legislator must also assess whether persons who can plausibly demonstrate that they may have been affected by surveillance measures can be granted the right to initiate such oversight measures. Within the framework of the oversight regime in question here, which does not give effect to the constitutional guarantee of legal protection and has no bearing on the possibility of having formal recourse to the courts pursuant to §§ 40 and 50(1) no. 4 VwGO, the Constitution does not preclude the design of oversight as a procedure that at least partially excludes affected persons and the public (*in camera*). This applies at least where the exclusion of affected persons and the public is necessary to allow for oversight which would otherwise not be possible at all and would therefore not be required under constitutional law (regarding such complaint proceedings under the law of the United Kingdom cf. Leigh, in: Dietrich/Sule [eds.], Intelligence Law and Policies in Europe, 2019, p. 553 <575 *et seq*.>; see also the considerations 280

on whether applicants are to be considered victims and on the availability of domestic legal remedies in ECtHR, Big Brother Watch and Others v. the United Kingdom, Judgment of 13 September 2018, no. 58170/13 and others, §§ 249 *et seq*.).

d) It must be guaranteed that oversight can be exercised continually and is institutionally independent. This includes that the oversight bodies must have a separate budget and independent management of their personnel, except where the appointment of the members of the panel resembling a court and the directors of the oversight bodies is concerned. The bodies must be effectively shielded from external influence and must be completely independent in this regard. 281

For the rest, the legislator is afforded wide latitude as regards the institutional structure of the oversight bodies. For example, this concerns the question of whether administrative oversight should be exercised by the Federal Data Protection Commissioner or by an independent oversight body. However, the legislator will have to organise oversight in such a way that it is not obstructed by the third party rule (see para. 292 *et seq*. below). It is not predetermined by the Constitution whether oversight resembling judicial review and administrative oversight should be combined under one roof in a single institution, which would incorporate the panels resembling courts into a comprehensive oversight body – whilst ensuring their members' independence, which must be equivalent to judicial independence –, or whether the two types of oversight should be exercised by two independent bodies. Yet the legislator is required to establish clear institutional structures. 282

e) Overall, the oversight bodies must be equipped with resources that allow for the effective and independent performance of their tasks. 283

aa) The oversight bodies must be equipped with competent and professional personnel and their composition must be balanced. In this respect, too, the legislator has wide latitude, but it is obliged to ensure that the legislative design guarantees effective oversight that is independent in legal and factual terms. 284

(1) The legislator must require the appointment of persons that are experts in the field, can fully understand the processes within the Federal Intelligence Service and ensure independent and competent oversight when they work together. At least with regard to administrative oversight, it may be necessary to not only consider legal experts, but also persons with other knowledge particularly in the field of information technology. 285

(2) With regard to oversight resembling judicial review, it must be ensured that the appointed members are independent in a way that is equivalent to judicial independence. In particular, they must not be bound by instructions and must be appointed for a sufficiently long and fixed term. As regards the composition of the panel, the judicial perspective must be accorded significant weight, which must be ensured through the appointment of a large proportion of members with longstanding judicial experience. This does not mean that other legal professionals cannot be appointed, 286

too. It must be taken into consideration that other expertise, in particular technical expertise, may also be helpful to the panel. It is for the legislator to decide whether the members of the oversight body resembling a court should also include non-lawyers – possibly depending on the type of decision to be made –, or whether it wants to provide the body with other possibilities for drawing on technical expertise.

(3) Overall, it must be ensured that oversight is competent and professional by generally appointing persons to the oversight body for whom this is their primary occupation; oversight that is mostly exercised in an honorary capacity is not sufficient. The composition of the oversight bodies must also be balanced. Both structurally and in terms of personnel, a sufficient distance to the Federal Intelligence Service must be ensured to guarantee the independence required of the oversight bodies. 287

bb) Sufficient personnel and resources must be made available for both types of oversight. The oversight body resembling judicial review requires a sufficient number of positions and panels to thoroughly conduct the oversight tasks assigned to it; the financial resources available for the positions must be sufficient to attract highly qualified persons. Likewise, the administrative oversight body requires a sufficient number of positions for qualified personnel. Financial resources must be sufficient to permit effective scrutiny of, for example, the filtering mechanisms used to remove communications in which Germans and persons within Germany are involved or which concern relationships of trust; to this end, the oversight bodies must be able to develop their own databases and software where necessary. The positions and resources to be allocated to each oversight body will probably be more or less equivalent to what is currently allocated to the Permanent Representative of the Parliamentary Oversight Body. 288

f) The oversight bodies must have all the powers necessary for effective oversight vis-à-vis the Federal Intelligence Service. 289

aa) Both oversight bodies must be granted comprehensive access to all documents. The legislator must impose an obligation on the Federal Intelligence Service to support the oversight bodies in the performance of their tasks, to provide information to them and to grant them access to documents and files, information about its software and access to its premises at all times (cf. BVerfGE 133, 277 <370 and 371 para. 215 *et seq*.>; 141, 220 <284 and 285 para. 141>; see also BTDrucks 14/5655, p. 26 with reference to BVerfGE 100, 313 <401>). The oversight bodies can determine their procedures and select their methods themselves insofar as these are not provided for by law. 290

bb) As part of the constitutional requirements with regard to oversight, the Federal Intelligence Service must document its data processing measures (cf. BVerfGE 133, 277 <370 para. 215>; 141, 220 <284 and 285 para. 141>; established case-law). The various steps of surveillance must be documented in a way that makes effective oversight possible. Where necessary, the relevant principles must be determined in more detail by the Federal Intelligence Service in consultation with the oversight bodies. 291

cc) Oversight must not be obstructed by the third party rule. In designing the oversight bodies and setting out requirements regarding agreements between the Federal Intelligence Service and other intelligence services, the legislator must ensure that the Federal Intelligence Service cannot prevent oversight by invoking the third party rule. 292

Nevertheless, the third party rule is a rule of conduct that is based on agreements with foreign intelligence services and generally recognised by all intelligence services; according to this rule, based on informal arrangements, intelligence obtained from foreign intelligence services may not be shared with third parties without the consent of the intelligence service in question (cf. BVerfGE 143, 101 <150 para. 162; 151 para. 164>). The Federal Government can also invoke this rule, insofar as it has given assurances on the basis of which intelligence was shared by a foreign intelligence service and the question of whether this intelligence can be shared with “third parties” arises; for example, the Federal Government refused to provide certain information to a committee of inquiry of the *Bundestag*, i.e. a third party, on the grounds that it had given such assurances to the United States of America (cf. BVerfGE 143, 101 <152 para. 167; 155 *et seq*. para. 176 *et seq*.>). 293

The bodies conducting the constitutionally required comprehensive oversight of the Federal Intelligence Service must be designed as independent oversight bodies that are strictly committed to secrecy and not integrated into Parliament and its political communication channels, so as to ensure that the third party rule cannot provide grounds for refusing to cooperate with them. There is no general definition setting out whether an oversight body must be considered a “third party” within the meaning of the third party rule; rather, this is determined on the basis of its organisational design and agreements between intelligence services (cf. BTDrucks 18/12850, pp. 98 and 99). The third party rule is an administrative practice that is not legally binding, but is merely based on agreements with other intelligence services; it is thus flexible and the Federal Government can influence its practical significance ([…]). The Federal Government and the Federal Intelligence Service do remain bound by the assurances they have given. However, in the future, it must be ensured, through the way the oversight bodies are designed and through changes in agreements with foreign services, that the bodies conducting legal oversight are no longer considered “third parties” (cf. also European Commission for Democracy through Law [Venice Commission], Report on the Democratic Oversight of Signals Intelligence Agencies, CDL-AD[2015]011, p. 5 [no. 13]; Council of Europe, Parliamentary Assembly, Resolution 1838 [2011], p. 2 [no. 7]; Council of Europe, Commissioner for Human Rights, Democratic and effective oversight of national security services, 2015, p. 13 [Recommendation no. 16]). 294

On the one hand, it must be guaranteed that, despite the third party rule, constitutionally required oversight also extends to the Federal Intelligence Service’s handling of information obtained from foreign intelligence services; on the other hand, the Federal Intelligence Service must be able to continue to cooperate with other intelligence 295

services (see paras. 246 and 247 above), which is especially important for safeguarding the Federal Republic of Germany's interests with regard to foreign and security policy. The practice of other intelligence services shows that this is possible; their oversight bodies have full access to all documents necessary to scrutinise the intelligence services that are subject to their oversight (regarding the rights to information granted to the Investigatory Powers Tribunal in the United Kingdom cf. ECtHR, Big Brother Watch and Others v. the United Kingdom, Judgment of 13 September 2018, no. 58170/13 and others, §§ 250, 379; regarding the Investigatory Powers Commissioner's unlimited rights to information see Annual Report of the Investigatory Powers Commissioner 2017 of 31 January 2019, p. 41).

dd) Oversight can in principle be subject to strict secrecy rules. Secrecy can be accorded significant weight not only when it comes to the premises of oversight bodies and their technical resources, but also when it comes to choosing their personnel. In particular, secrecy can be ensured through the imposition of confidentiality requirements that are subject to effective sanctions. 296

(1) However, open and direct exchange between the oversight bodies must be guaranteed (cf. BVerfGE 133, 277 <370 para. 216>). The requirement of effective and coherent oversight calls for such exchange given that these bodies, which are subject to the same confidentiality requirements, are together responsible for oversight of the same measures. Where structural problems become apparent in the context of oversight or differences with the Federal Intelligence Service arise that cannot be resolved otherwise, it must be possible to raise concerns with the head of the Federal Intelligence Service and, if necessary, the head of the Federal Chancellery, which exercises supervision; these must then take action where necessary. 297

(2) Yet the flow of information to the parliamentary sphere and thus also to the Parliamentary Oversight Body can in principle be limited on grounds of secrecy. The legislator may take into account that parliamentary oversight differs (see para. 300 below) from oversight that merely serves to ensure that the law is observed, and that secrecy in the parliamentary and political sphere is subject to factual limits. Nonetheless, under Art. 45d GG, the Parliamentary Oversight Body must regularly be informed about oversight activities in a manner that maintains secrecy. In addition, the oversight bodies must also be able to ultimately take their objections and their criticism to Parliament and thus to the public in an abstract manner that guarantees secrecy. 298

(3) The effectiveness of oversight must be continually monitored given that oversight processes largely take place without Parliament and the public obtaining knowledge thereof, but are potentially in conflict with the Federal Intelligence Service's work that is based on secrecy, and given that the conditions under which surveillance measures and oversight take place can change quickly in light of technological developments. The effectiveness of oversight in practice and of its statutory framework must be evaluated at regular intervals (regarding evaluation duties cf. also BVerfGE 299

150, 1 <90 para. 176>).

g) The design of oversight conducted by the Parliamentary Oversight Body and its Permanent Representative, which exists alongside the other oversight bodies, is also determined by the legislator; this body can become involved in the oversight of surveillance measures (cf., e.g., § 14 of the Article 10 Act). Such oversight is not at issue in the present proceedings. The oversight conducted by the Parliamentary Oversight Body serves a separate purpose that is not limited to ensuring adherence to the law and respect for fundamental rights. It is a manifestation of general parliamentary responsibility for the proper and politically adequate performance of tasks by the executive ([…]). Requirements regarding its design cannot be derived from the fundamental rights invoked in the present proceedings; parliamentary powers vis-à-vis the executive that are derived from the Constitution remain unaffected by the requirements set out above (cf. in this respect BVerfGE 143, 101). 300

VI.

Based on the requirements set out above, the challenged provisions also do not satisfy the constitutional requirements in substantive terms. As with the violation of the requirement to expressly specify affected fundamental rights (see paras. 134 and 135 above), the provisions are based on the assumption, which is incorrect from a constitutional law perspective, that fundamental rights are not applicable to the surveillance powers in question. Given that the provisions are unconstitutional for formal reasons alone, the substantive review will only address their key shortcomings. A new legal framework for the Federal Intelligence Service's powers will have to accommodate the fundamental rights of the persons whose telecommunications are under surveillance and will thus have to adhere to the requirements set out above. 301

1. The provisions on data collection and processing in §§ 6 and 7 BNDG are incompatible with Art. 10(1) GG and the proportionality requirements arising from it. 302

a) Firstly, this applies to strategic surveillance carried out from within Germany pursuant to § 6 BNDG. 303

aa) § 6 BNDG already fails to satisfy the constitutional requirements in respect of interferences with fundamental rights of Germans and persons within Germany which result from foreign surveillance and cannot be avoided for technical reasons. In particular, it does not sufficiently set out that filtering is necessary and the requirements such filtering must satisfy (see para. 170 *et seq*. above). The substantive prohibition in § 6(4) BNDG alone, which is misleading in implying that the collection of data concerning German citizens and persons within Germany could be avoided entirely, does not satisfy these requirements. Moreover, there are no clear statutory provisions on the required immediate deletion of domestic communications that were intercepted unintentionally. While § 10(4) first sentence BNDG does provide for such deletion in principle, it cannot be inferred from § 10(4) second to sixth sentence BNDG whether and to what extent the Federal Intelligence Service can refrain from deleting such 304

communications (cf. Hölscheidt, Jura 2017, p. 148 <156>).

bb) Furthermore, the surveillance measures conducted pursuant to § 6 BNDG are not limited to precisely defined and weighty purposes (see paras. 175 and 176 above). The broad and openly worded purposes listed in § 6(1) first sentence BNDG, which, according to the explanatory memorandum to the draft act, are not intended to narrow down the Federal Intelligence Service's tasks in any way (cf. BTDrucks 18/9041, p. 22), clearly fail to meet this requirement. In particular, a statutory restriction of the purposes cannot be replaced by the Mission Statement of the Federal Government, which is solely based on political considerations (cf. in this respect United Nations Office of the High Commissioner for Human Rights, letter of the Special Rapporteurs of 29 August 2016, OL DEU 2/2016, p. 5). 305

Consequently, surveillance is not structured along the lines of formal determinations of precisely delimited surveillance measures, which must adhere to the principle of proportionality and must, in a verifiable manner, inform the selection of the transmission routes to be intercepted and of the search terms to be used as well as further data processing and use (see para. 178 *et seq*. above; […]). Moreover, statutory requirements regarding the use of search terms targeting specific individuals (see para. 185 *et seq*. above) and confidentiality protection of relationships of trust (see para. 193 *et seq*. above; […]) are lacking. § 11 BNDG affords insufficient protection of the core of private life (see para. 203 *et seq*. above). 306

Nor does the law sufficiently determine how the data obtained by means of strategic foreign surveillance may be analysed (see para. 192 above). As a merely generalised provision on data processing by the Federal Intelligence Service, § 19 BNDG does not satisfy the requirements in this regard. The provision is disproportionate given that it is unspecific and merely refers, in a broad and general manner, to §§ 10 and 11 BVerfSchG as the basis for processing, altering and using data collected pursuant to §§ 6 and 7 BNDG. 307

cc) Insofar as § 6 BNDG is meant to also provide a basis for collecting other personal data of German citizens, German legal entities or persons within Germany to which Art. 10 GG does not apply (cf. BTDrucks 18/9041, p. 24), the provision lacks the required legal clarity (see para. 137 *et seq*. above). The provision does not even make it clear that it is to serve as a basis for using data not protected by the privacy of telecommunications; it also fails to set out which data is to be collected for what use as well as on what basis and with regard to which fundamental rights the legislator considers this to be justified. 308

b) Secondly, § 7 BNDG, which governs the further processing of data obtained from other states by means of foreign surveillance as well as certain limits to such data collection, is also not compatible with Art. 10(1) GG. The provision is based on the incorrect assumption that a statutory basis authorising such data collection is not necessary and that such data can be collected on the basis of § 1(2) BNDG alone, which merely lays down the Federal Intelligence Service's tasks. Yet such data collection, 309

too, is impermissible without a sufficient statutory authorisation (see paras. 87 *et seq*. and 120 above). § 7 BNDG is unconstitutional in itself given that it implies that data collection is permissible, only restricts it in some cases and otherwise allows for further processing of data without any restrictions. As a separate (implicit) authorisation to collect data, it does not satisfy the constitutional requirements applicable to such a statutory basis set out above. Yet as shown above, the legislator did not intend § 7 BNDG to be a statutory basis authorising data collection at all. Therefore, § 7 BNDG violates Art. 10(1) GG in that it governs the processing of data which, in the absence of a constitutional statutory basis, should not have been collected at all and in respect of which further processing is therefore also impermissible. Moreover, the provision is misleading in implying that such data may be collected and thereby provides legitimacy in respect of data collection that lacks a constitutional statutory basis.

2. The provisions on data sharing do not satisfy the constitutional requirements either. In part, they do not satisfy the requirement of legal clarity. For the rest, the provisions do not sufficiently limit data sharing to the purposes of protecting particularly weighty legal interests and prosecuting particularly serious criminal acts, nor do they make data sharing contingent upon the existence of sufficient indications of an identifiable danger or a suspicion, supported by specific facts, that such criminal acts have been committed. 310

a) § 24(1) first sentence BNDG, which concerns data sharing with domestic authorities, does not satisfy the requirement of legal clarity and specificity (see paras. 137 *et seq*. and 212 *et seq*. above). First of all, this is true to the extent that the provision generally allows the Federal Intelligence Service to share data “to perform its tasks”. In principle, a reference to tasks defined elsewhere is not incompatible with the requirement of legal clarity. However, such a general reference to the entire range of tasks of the Federal Intelligence Service – which do not encompass operational tasks, but are limited to gathering and analysing intelligence (cf. § 1(2) BNDG) – does not clearly determine for which purposes the provision allows data sharing (see para. 215 above). This was confirmed by the uncertainties expressed on this point in the oral hearing. The provision also lacks specificity insofar as it allows data sharing if the recipient needs the data for significant public security purposes. Given that it is not clear whether this encompasses any authority tasked with the enforcement of the general or specific law on maintaining public security and order or only specific security authorities, it cannot be clearly ascertained which authorities may receive data in the context of such sharing. For the rest, both provisions on data sharing do not satisfy the requirements regarding the necessary thresholds and regarding a qualified protection of legal interests (see para. 220 *et seq*. above). The unspecific reference to “significant” public security purposes, which is meant to exclude matters that are merely trivial (cf. regarding the identical wording in § 19(1) second sentence BVerfSchG BTDrucks 18/4654, p.34), is not sufficient. 311

b) § 24(3) BNDG in conjunction with § 20(1) first and second sentence BVerfSchG, which authorises the sharing of information with police authorities and public prose- 312

cution offices in the context of offences against state security, is also not compatible with the constitutional requirements. The provision does sufficiently specify which authorities may receive information, yet it is doubtful whether its multi-level chain of references satisfies the requirement of legal clarity (see para. 215 above). Regardless of these considerations, the requirements regarding the protection of legal interests are not met consistently (see para. 221 above). This is because not all of the criminal offences listed in §§ 74a and 120 of the Courts Constitution Act (*Gerichtsverfassungsgesetz* – GVG) and referenced, in a general manner, by § 24(3) BNDG in conjunction with § 20(1) first and second sentence BVerfSchG can be classified as particularly serious offences. The same applies to the openly-worded provision on data sharing, according to which any other offence may provide grounds for such sharing because of its aims or the offender's motive alone. Moreover, the provision does not determine the required threshold for data sharing in a sufficiently specific manner (see paras. 213 *et seq.,* 220 *et seq.* as well as 227 and 228 above). In this respect, the legislator must set out prerequisites which require that there be indications of an identifiable danger (cf. BVerfGE 141, 220 <271 *et seq*. para. 111 *et seq*.>) or facts which provide sufficient grounds for suspicion.

c) § 24(2) first sentence BNDG in conjunction with § 19(4) BVerfSchG, which governs data sharing with "other" – mainly private – bodies, does not satisfy the requirements of Art. 10(1) GG in every respect. Yet the provision does not lack specificity, nor is the protection of legal interests it aims to achieve objectionable. The reference to the "protection of the free democratic basic order, the existence and security of the Federation or of a *Land*" and to "the guarantee of the security of vital facilities or facilities that must be defended pursuant to § 1(4) of the Security Clearance Check Act (*Sicherheitsüberprüfungsgesetz*)" is unambiguous in the context of the understanding of these terms in other areas and refers to legal interests of particular weight. Again, however, it is doubtful whether the multi-level chain of references in the provision satisfies the requirement of legal clarity (see para. 213 *et seq*. above). In any case, a threshold for data sharing is lacking (see paras. 216 *et seq*. and 222 above). 313

d) § 24(2) first sentence BNDG in conjunction with § 19(2) BVerfSchG is also unconstitutional. This provision allows information to be shared with NATO troops stationed in Germany; it refers to Art. 3 of the Agreement to Supplement the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces with respect to Foreign Forces stationed in the Federal Republic of Germany of 3 August 1959 (BGBl 1961 II p. 1218). The provision lacks the necessary legal clarity and specificity (see paras. 137 *et seq*. and 213 *et seq*. above). Its three-part chain of references refers to an international treaty provision, which in itself merely provides a general framework for cooperation in a broad and open manner. It cannot be ascertained from that chain of references with sufficient clarity and specificity for what purpose information may be shared. Moreover, the provision does not limit data sharing to the protection of legal interests of sufficient weight, nor does it provide for thresholds for data sharing (see para. 220 *et seq*. above). Making the permissibility of data 314

sharing contingent on its “necessity” is not sufficient.

e) Finally, § 24(2) first sentence BNDG in conjunction with § 19(3) BVerfSchG, which governs the sharing of data with foreign public bodies, does not satisfy the constitutional requirements in several respects. 315

The provision does not contain a sufficiently precise determination of the authorities that may receive data, which also cannot be determined by looking at the openly-worded purposes for which data may be shared (see paras. 137 *et seq*. and 213 *et seq*. above; cf. in this respect BVerfGE 130, 151 <203>; 133, 277 <337 and 338 para. 143>; 141, 220 <334 para. 306>). Furthermore, the provision does not limit data sharing to sufficiently qualified legal interests, nor does it provide for a threshold for data sharing (see para. 220 *et seq*. above). 316

It also does not impose a clear obligation on the Federal Intelligence Service to ascertain that the data shared by it is handled in accordance with the rule of law. There are some elements of such an obligation in § 19(3) second sentence BVerfSchG. However, this does not satisfy the requirements set out above (see para. 233 *et seq*. above). The provision does not expressly state the need to ascertain that a minimum level of protection is guaranteed under data protection law (see para. 235 *et seq*. above) and it lacks documentation requirements (see para. 229 above). Moreover, it does not specifically accommodate confidentiality protection of relationships of trust (see para. 240 and para. 193 *et seq*. above). 317

§ 31 BNDG in conjunction with § 23 no. 1 BVerfSchG does not sufficiently ensure the required ascertainment. It is not clear from that provision that the authority sharing the data must actively ascertain what the circumstances in the receiving state are – both in terms of data protection law and in terms of human rights guarantees –, document this ascertainment and investigate any doubts (see para. 233 *et seq*. above). The provision also does not rule out that key aspects of the rule of law are disregarded in a balancing of interests (see para. 237 above). 318

f) In an overall assessment, the provisions on data sharing do not satisfy the constitutional requirements. These provisions are, for the most part, based on the structure of the Federal Protection of the Constitution Act and other security laws that are older and have not sufficiently been adapted to developments in the case-law. Moreover, in formal terms, none of the provisions on data sharing contain an obligation to document data sharing (see para. 229 above) and to specify its statutory basis (see para. 229 above). 319

3. The legal framework on cooperation in §§ 13 to 15 BNDG is also not compatible with the proportionality requirements arising from Art. 10(1) GG and is thus unconstitutional in both formal and substantive terms. 320

a) The constitutional shortcomings identified in respect of § 6 BNDG apply to these provisions as well. Data collection and processing in the context of cooperation is not based on sufficiently clear provisions requiring that telecommunications data of Ger- 321

mans and persons within Germany be removed (see paras. 176 *et seq*. and 253 above). Nor are surveillance measures in the context of cooperation limited to weighty purposes that are sufficiently specified by law (see paras. 175 and 176 and 253 above); § 13(4) BNDG does not sufficiently limit the purposes in such a way. Therefore, the permissibility of cooperation is not tied to intelligence aims that must be specified in relation to each measure, and is not structured along the lines of such aims (see paras. 178 *et seq*. and 253 above).

b) Insofar as § 14(1) BNDG provides a legal basis according to which data collected by the Federal Intelligence Service may be analysed by means of search terms determined by foreign services, no sufficient obligations to check the search terms are imposed [on the Federal Intelligence Service]. In particular, safeguards to protect persons meriting special protection and relationships of trust are lacking (see paras. 194 *et seq*. and 257 above). Apart from that, it is sufficient in substantive terms that search terms may only concern the aims of cooperation, must afford protection from targeted interception of persons in the European Union and be compatible with the Federal Republic of Germany's interests (cf. § 14(1) first and second sentence and § 14(2) BNDG). However, there are no procedural safeguards that sufficiently guarantee the existence of a statutory obligation to check whether search terms provided by foreign services are permissible in substantive terms based on a minimum of information to be disclosed by the foreign services, and to subject random samples to manual screening where necessary (see para. 254 *et seq*. above). 322

c) Automated data sharing pursuant to § 15(1) BNDG is also not subject to sufficiently strict provisions requiring the removal of data of persons who merit special protection or data stemming from special relationships of trust (see paras. 194 *et seq*. and 257 above). The law also does not require with sufficient legal clarity that the recipients provide assurances that they will respect relationships of trust and prohibitions of discrimination or adhere to basic thresholds for data sharing (see para. 260 above). The abstract and general assurance pursuant to § 13(3) no. 4 BNDG that data will be used in line with the principles arising from the rule of law is not sufficient in this respect. The law also does not provide for a sufficient ascertainment that the recipient will use the data in accordance with the rule of law (see paras. 233 *et seq*. and 261 above). Finally, the provision does not restrict the sharing of unfiltered traffic data in any way (see para. 262 *et seq*. above) 323

4. Moreover, it is clearly evident that the Federal Intelligence Service Act does not set out a sufficient legal framework for oversight of the aforementioned powers. The very limited obligations to provide information that are set out in § 22 BNDG and the lack of notification requirements vis-à-vis affected persons abroad in relation to the surveillance of foreign communications are not objectionable in themselves. However, comprehensive independent oversight is required to compensate for the broad scope of the provisions and the very limited possibilities of obtaining legal protection in practice – as set out above (see para. 267 *et seq*.). As the law currently stands, in view of their powers and their organisational and institutional design, the Independent 324

Body and the Federal Data Protection Commissioner cannot ensure such oversight in the constitutionally required form.

VII.

325 Insofar as the provisions authorise surveillance measures targeting journalists and thus give rise to interferences with Art. 5(1) second sentence GG, they are also incompatible with the Constitution, since they do not sufficiently meet the specific needs for protection of independent foreign journalists (cf. in this respect United Nations Office of the High Commissioner for Human Rights, letter of the Special Rapporteurs of 29 August 2016, OL DEU 2/2016, pp. 5 and 6).

F.

326 Contrary to the complainants' view, no further requirements derive from the fundamental rights of the European Union, notwithstanding the question to what extent the competence to conduct such a review in the case at hand falls to the Federal Constitutional Court. Even if, in light of Art. 15 of Directive 2002/58/EC, the challenged provisions were in part considered to be implementing EU law within the meaning of Art. 51(1) first sentence of the Charter of Fundamental Rights of the European Union, there would be no specific and sufficient indication that the fundamental rights of the Basic Law, in the interpretation set out here, do not simultaneously ensure the level of protection of the Charter according to the CJEU's case-law (cf. BVerfG, Order of the First Senate of 6 November 2019 - 1 BvR 16/13 -, para. 67 *et seq*. – Right to be forgotten I). In particular with regard to the power to retain and analyse traffic data, such indication does not follow from the CJEU's decisions concerning the Data Retention Directive (Judgment of 8 April 2014, Digital Rights Ireland and Seitlinger and Others, C-293/12, C-594/12, EU:C:2014:238) and concerning data retention powers of the Member States (Judgment of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970). Those decisions concern the domestic interception of telecommunications traffic data in its entirety, which makes it possible to compile almost complete personality profiles of individual communication participants. This differs fundamentally from powers to collect a limited volume of traffic data stemming from foreign communications and selected networks – which generally does not allow for the interception of all parts of the communication relations of affected persons. Therefore, in the context of a European regime of fundamental rights protection that seeks to accommodate diversity, it is not ascertainable that the fundamental rights of the Basic Law do not simultaneously ensure the level of protection of the Charter of Fundamental Rights.

G.

I.

327 In light of the foregoing, §§ 6, 7 and 13 to 15 BNDG are unconstitutional. Insofar as they concern data collected on the basis of the aforementioned provisions, §§ 19,

24(1) first sentence, 24(2) first sentence and 24(3) BNDG are also unconstitutional. They violate the fundamental rights under Art. 10(1) GG of complainants nos. 2 to 8 and the fundamental rights under Art. 5(1) second sentence GG of complainants nos. 2 to 7. Thus, there is no longer a basis for applying §§ 9 to 11, 16, 19, 20, 22, 32 and 32a BNDG, which do not sufficiently satisfy the requirements according to which they must provide for proportionate limits, in line with the rule of law, to the powers that are being declared unconstitutional.

328 There is no need to determine whether the challenged provisions violate the fundamental rights of complainant no. 1 as a legal entity based in an EU Member State. The declaration of incompatibility with the Basic Law, which has the force of law pursuant to § 31(2) second sentence BVerfGG, provides the legal protection sought by complainant no. 1, at least in substance and to the same extent as could be achieved if complainant no. 1 were considered a holder of fundamental rights.

II.

329 The finding that a statutory provision is unconstitutional generally results in a declaration that it is void. However, pursuant to § 31(2) second and third sentence BVerfGG, the Federal Constitutional Court can choose to declare only that an unconstitutional provision is incompatible with the Basic Law (cf. BVerfGE 109, 190 <235>). It then merely objects to the unconstitutional provision without declaring it void. The Court may combine the declaration of incompatibility with an order to continue to apply the unconstitutional provisions for a limited time. This may be considered in cases where the immediate invalidity of the objectionable provision would eliminate the basis for the protection of exceptionally significant public interests and if the outcome of a balancing of these interests against the affected fundamental rights requires that the interference be tolerated for a transitional period (cf. BVerfGE 33, 1 <13>; 33, 303 <347 and 348>; 40, 276 <283>; 41, 251 <266 *et seq*.>; 51, 268 <290 *et seq*.>; 109, 190 <235 and 236>).

330 This is the case here. Depending on the political situation, the objectionable powers may become very important for the security of the Federal Republic of Germany and as a basis for action of the Federal Government, and this may happen quite rapidly, especially when taking into account the potential dynamics of threats in light of the realities of information technology. A declaration of incompatibility or a temporary order of suspension would thus involve considerable risks. Moreover, an unexpected suspension of the possibility to cooperate with other intelligence services might damage trust in the Federal Intelligence Service as a reliable partner, possibly in the long term. It must also be taken into account that the general structure of the objectionable powers can be designed in a manner that is constitutionally tenable, and that their shortcomings can thus be remedied. It is true that remedying the statutory basis of these powers requires fundamental amendments, given that the new provisions must provide a basis for surveillance measures that takes into account Art. 10(1) GG and must thus create novel limits and checks in accordance with the rule of law. However,

in light of the great importance that the legislator may accord to foreign surveillance, an order to continue to apply the unconstitutional provisions for a limited time is preferable to the immediate invalidity of the provisions until new provisions have been enacted, which is expected to happen in the foreseeable future.

The legislator must enact new provisions by 31 December 2021 at the latest. The order of continued application is only valid until that date. 331

III.

[…] 332

Harbarth Masing Paulus

Baer Britz Ott

Christ Radtke

Bundesverfassungsgericht, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17

Zitiervorschlag BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 - Rn. (1 - 332), http://www.bverfg.de/e/rs20200519_1bvr283517en.html

ECLI ECLI:DE:BVerfG:2020:rs20200519.1bvr283517