Headnotes

to the Judgment of the First Senate of 26 April 2022

- 1 BvR 1619/17 -

(Bavarian Protection of the Constitution Act)

1. **Under the currently applicable legal framework, domestic intelligence services have specific surveillance and intelligence gathering responsibilities and do not have the operational follow-up powers that police authorities do. In principle, this can justify linking the use of their surveillance powers to modified thresholds for interference with fundamental rights. However, strict requirements must then be applied to the sharing of any personal data and information obtained as a result.**

2. **The strictness of the proportionality requirements that apply to the covert surveillance measures of a domestic intelligence service depends on the severity of interference resulting from the measure in question.**

a. **Measures that could lead to extensive insight being gained into one's personality are subject to the same proportionality requirements as police surveillance.**

b. **In other cases, the surveillance powers of a domestic intelligence service do not have to be linked to the presence of danger as they do for police action. However, a sufficient need for surveillance specifically relating to the protection of the constitutional order is then required. Such a need only arises if the surveillance measure in question is necessary in the individual case to investigate a specific endeavour that warrants surveillance by an intelligence service and if sufficient factual indications support the need for surveillance. The greater the severity of interference resulting from the surveillance measure, the more urgent this need for surveillance must be. The legislator must set forth in a sufficiently specific and clear manner what level of need for surveillance is required in each case. Special requirements apply when persons are affected by the surveillance who are not themselves part of the endeavour at issue or otherwise acting in furtherance of the endeavour. Depending on the severity of interference resulting from the measure to be carried out, *ex ante* oversight of the measure by an independent body may be necessary.**

3. **The sharing of personal data and information by domestic intelligence services with other bodies constitutes a separate interference with fundamental rights. If the data was collected using intelligence service methods, the justification for the interference resulting from the sharing of such data must be assessed according to the criterion of a hypothetical recollection of the data. Based on this criterion, the question of whether the receiving authority is permitted to receive such data depends on whether the receiving authority could have been permitted to collect the same data and information itself for the purpose for which the data is being shared, using comparably intrusive methods as the domestic intelligence service's original surveillance. Domestic intelligence services are only permitted to share data with other bodies in order to protect particularly weighty legal interests. The threshold for data sharing differs according to which body the data is shared with.**

   a) Data sharing with a public security authority must serve to protect a particularly weighty legal interest for which there is at least a sufficiently identifiable danger.

   b) Data sharing with a prosecution authority may only be considered for the purpose of prosecuting particularly serious criminal offences and requires a suspicion based on specific facts and supported by sufficiently concrete and tangible circumstances.

   c) Data sharing with any other body is only permissible to protect a particularly weighty legal interest. The constitutional requirements applicable to the threshold for data sharing differ according to the severity of interference, which depends among other things on the operational follow-up powers of the receiving authority. Data sharing with another domestic intelligence service is possible if there are sufficient factual indications to suggest that the information is required in that particular case to investigate a specific activity or group that warrants surveillance by an intelligence service.

   d) The same requirements that apply to data sharing with bodies in Germany also apply to data sharing with other states. Furthermore, the receiving state must handle the shared data in accordance with basic human rights and data protection standards, and such compliance must be ascertained accordingly.

4. **The principle of legal clarity sets limits to the use of chains of statutory references in legislation. Confusing, multi-level chains of statutory references are incompatible with fundamental rights requirements.**

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 1619/17 -

Pronounced
on 26 April 2022
Langendörfer
Tarifbeschäftigte
as Registrar
of the Court Registry

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaint

[of 3 complainants]

– authorised representatives: 1. Prof. Dr. Matthias Bäcker, LL.M.,

authorised representative for nos. 1 to 3

2. Rechtsanwalt David Werdermann, LL.M.,

authorised representative for no. 2

3. Rechtsanwalt Dr. Bijan Moini,

authorised representative for no. 3 –

against Article 8a(1) first sentence no. 1, second to fifth sentence, Article 8b(2) first sentence nos. 2 and 3, Article 8b(3), Article 9, Article 10(1), Article 11(2) third sentence, Article 12(1), Article 15(2) and (3), Article 16(1), Article 17(2) first sentence, Article 18(1), Article 19(1), Article 19a(1) and (3) first and fourth sentence, Article 20(1), Article 23(1) first sentence, Article 23(1) third sentence nos. 1 and 2, Article 25(1), Article 25(1a), Article 25(2) first sentence nos. 2 and 3, Article 25(2) second sentence, Article 25(3) first sentence nos. 2 and 3 of the Bavarian Protection of the Constitution Act (*Bayerisches Verfassungsschutzgesetz*) of 12 July 2016, last amended by § 3 of the Act of 23 July 2021 (Bavarian Law and Ordinance Gazette, *Bayerisches Gesetz- und Verordnungsblatt*, page 418)

the Federal Constitutional Court - First Senate -

with the participation of Justices

President Harbarth,

Paulus,

Baer,

Britz,

Ott,

Christ,

Radtke,

Härtel

held on the basis of the oral hearing of 14 December 2021:

Judgment

1. **Article 15(3) of the Bavarian Protection of the Constitution Act of 12 July 2016 (Bavarian Law and Ordinance Gazette, page 145), last amended by § 3 of the Act Amending the Bavarian Police Act and Other Statutory Provisions of 23 July 2021 (Bavarian Law and Ordinance Gazette, page 418), violates Article 10(1) of the Basic Law (*Grundgesetz*) and is void.**

2. **Article 9(1) first sentence, Article 10(1), Article 12(1), Article 18(1), Article 19(1), Article 19a(1), Article 25(1) no. 1 second alternative, Article 25(1) no. 3, Article 25(1a), Article 25(2) first sentence nos. 2 and 3, Article 25(3) first sentence no. 2, Article 8b(2) first sentence no. 2 and Article 8b(3) of the Bavarian Protection of the Constitution Act are incompatible with Article 2(1) in conjunction with Article 1(1), Article 10(1), Article 13(1) and (4) of the Basic Law.**

3. **Until the legislator has enacted new provisions, or until 31 July 2023 at the latest, the provisions that have been declared incompatible with the Basic Law continue to apply subject to the following conditions:**

Measures under Article 9(1) first sentence [*surveillance of private homes*] and Article 10(1) [*remote searches of information technology systems*] of the Bavarian Protection of the Constitution Act may only be taken for the purpose of averting an acute danger to the existence or security of the Federation or a *Land*, or to the life, limb or liberty of the person, or to assets the preservation of which is of special public interest, and then only in the event that suitable police assistance for the legal interest at risk cannot otherwise be timely obtained. In this respect, Article 8a(1) of the Bavarian Protection of the Constitution Act must be applied subject to the rebuttable presumption that intelligence obtained from the surveillance of a private home relates to the core of private life.

Technical means may not be deployed under Article 12(1) [*tracking of mobile devices*] of the Bavarian Protection of the Constitution Act in a way that allows the movements of a mobile device belonging to a person under surveillance to be tracked over a prolonged period.

Measures under Article 18(1) [*undercover officers*] and Article 19(1) [*informants*] of the Bavarian Protection of the Constitution Act must be terminated after a maximum of six months unless they are essential to investigate an endeavour aimed at committing particularly serious criminal acts that threaten the legal interests protected under § 3(1) of the Federal Protection of the Constitution Act (*Bundesverfassungsschutzgesetz*) […]. If the use of undercover officers or informants is directed against specific persons, Article 19a(2) of the Bavarian Protection of the Constitution Act must be applied accordingly.

Technical means for recording images and for intercepting and recording non-public spoken communication may not be covertly deployed under Article 19a(1) [*observation outside the home*] of the Bavarian Protection of the Constitution Act unless this is essential to investigate an endeavour aimed at committing particularly serious criminal acts that threaten the legal interests protected under § 3 of the Federal Protection of the Constitution Act and the other statutory requirements are satisfied.

Under Article 25 of the Bavarian Protection of the Constitution Act, the sharing of personal data and information obtained using intelligence service methods is only permissible to protect an exceptionally significant public interest; this is equivalent to limiting the sharing of such data to cases involving particularly serious criminal offences. Furthermore, the specific grounds for sharing the data must satisfy the applicable requirements as set forth in the reasons of this judgment.

4. **For the rest, the constitutional complaint is in part dismissed as inadmissible and in part rejected as unfounded.**

5. **[…]**

Table of contents

R e a s o n s:

A. Facts of the case

The constitutional complaint is directed at provisions contained in the Bavarian Protection of the Constitution Act (*Bayerisches Verfassungsschutzgesetz* – BayVSG) of 12 July 2016 (Bavarian Law and Ordinance Gazette, *Bayerisches Gesetz- und Verordnungsblatt* – BayGVBl p. 145; substantially amended by the Act of 12 June 2018, BayGVBl p. 382). These provisions set out the powers of the Bavarian *Land* Office for the Protection of the Constitution (*Bayerisches Landesamt für Verfassungsschutz*), i.e. the Bavarian domestic intelligence service. 1

I. Background of the challenged provisions

In July 2017, the complainants lodged a constitutional complaint challenging various provisions of the Bavarian Protection of the Constitution Act. The Bavarian legislator had significantly revised this law in 2016, restructuring the Bavarian *Land* Office's data collection powers, including its powers to collect data using intelligence service methods and to share data and information with other bodies. 2

The goal of the revision was to improve cooperation between the intelligence services, police and other security authorities. [...] 3

Shortly before the Bavarian Protection of the Constitution Act was revised, the Federal Constitutional Court issued its judgment on the Federal Criminal Police Office Act (Decisions of the Federal Constitutional Court, *Entscheidungen des Bundesverfassungsgerichts* – BVerfGE 141, 220). This prompted the Bavarian legislator to take further legislative action in the form of the Act Amending the Bavarian Protection of the Constitution Act (*Gesetz zur Änderung des Bayerischen Verfassungsschutzgesetzes*) of 12 June 2018 [...]. 4

The provisions of federal law to which the Bavarian Protection of the Constitution Act makes reference were themselves revised while the constitutional complaint proceedings were ongoing. [...] 5

II. Provisions relevant to the proceedings […]

The Bavarian Protection of the Constitution Act distinguishes between general powers of information processing in Art. 5 BayVSG, the specific power to collect information using intelligence service methods in Art. 8 BayVSG, and special intelligence service methods, which are specifically set out in Art. 9 to Art. 19a BayVSG. Art. 8b(1) BayVSG governs the processing of personal data. Data sharing, including the Bavarian *Land* Office's sharing of personal data with other bodies, is generally set out in Art. 25 BayVSG. Art. 8b(2) BayVSG contains specific rules for the processing of personal data obtained through the surveillance of private homes or remote searches of information technology systems. Art. 8b(3) BayVSG sets out special requirements for the processing of personal data obtained through special requests for information pursuant to Art. 15(2) and (3) and Art. 16(1) BayVSG. 6

[…] 7-39

III. The constitutional complaint

The complainants are members and, in some cases, active officials of organisations under surveillance by the Bavarian *Land* Office for the Protection of the Constitution and are also mentioned in its annual reports on the protection of the Constitution. They lodged a constitutional complaint in July 2017 challenging various data collection and data sharing powers set out in the Bavarian Protection of the Constitution Act. They claim that their fundamental rights under Art. 2(1) in conjunction with Art. 1(1), Art. 3(1), Art. 10(1), Art. 13(1) and Art. 19(4) of the Basic Law (*Grundgesetz* – GG) have been violated. […] 40

[…] 41-57

IV. Statements

Statements in respect of the constitutional complaint were submitted by the Bavarian *Landtag* (state parliament), the Bavarian *Land* Government and the Bavarian Data Protection Officer. 58

[…] 59-86

V. Oral *hearing*

The Federal Constitutional Court conducted an oral hearing on 14 December 2021. Statements were made by the complainants, the Bavarian *Landtag* (represented by the Chairperson of the Committee on Constitution, Legal and Parliamentary Affairs and Integration), the Bavarian *Land* Government (represented by the State Minister of the Interior, for Sport and Integration), and the Bavarian *Land* Office for the Protection of the Constitution. The Bavarian Data Protection Officer and the Society for 87

Civil Rights (*Gesellschaft für Freiheitsrechte e.V.*) were heard as expert third parties in accordance with § 27a of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz* – BVerfGG).

B. Subject matter and admissibility

I. Subject matter

1. […] 88

2. The constitutional complaint is ultimately directed at the surveillance powers conferred upon the Bavarian *Land* Office for the Protection of the Constitution under Art. 9(1) first sentence [*surveillance of private homes*], Art. 10(1) [*remote searches of information technology systems*], Art. 12(1) [*tracking of mobile devices*], Art. 15(2) and (3) [*information from service providers*; *disclosure of traffic data originating from data retention*], Art. 16(1) [*further information requests*], Art. 18(1) [*undercover officers*], Art. 19(1) [*informants*], Art. 19a(1) and (3) first and fourth sentence [*observation outside the home*] BayVSG, and the powers of data processing and sharing conferred under Art. 8b(2) first sentence no. 2, Art. 8b(3), Art. 25(1) nos. 1 and 3, Art. 25(1a), Art. 25(2) first sentence nos. 2 and 3, Art. 25(2) second sentence and Art. 25(3) first sentence nos. 2 and 3 BayVSG. 89

The complainants also regard several general provisions that concern procedural aspects of the surveillance framework as belonging to the subject matter of the proceedings (Art. 8a(1) first sentence no. 1, second to fifth sentence; Art. 11(2) third sentence; Art. 17(2) first sentence; Art. 20(1); Art. 23(1) first sentence, third sentence nos. 1 and 2 BayVSG). While these provisions are not directly challenged by the constitutional complaint, they may nonetheless be significant, especially for assessing the proportionality of the challenged powers (cf. BVerfGE 155, 119 <157 para. 64> - Subscriber data II; established case-law; see para. 132 below for further details). 90

[…] 91

II. Admissibility

The constitutional complaint is partly inadmissible because the complainants have failed to sufficiently demonstrate standing in respect of some of the challenged provisions, and because the requirements arising from the principle of subsidiarity in the broader sense have not been met in respect of some of the provisions. 92

[…] 93-141

III. European Union law

Some of the challenged provisions relate to data protection rules set out in directives and regulations of the European Union (cf. 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 <OJ EU, L 201 of 31 July 2002, p. 37 – ePrivacy Directive>; see in this regard CJEU, 142

Judgment of 6 October 2020, Privacy International, C-623/17, EU:C:2020:790, paras. 37 ff., 42; CJEU, Judgment of 6 October 2020, La Quadrature du Net, C-511/18, EU:C:2020:791, para. 96 f.; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA <OJ EU, L 119 of 4 May 2016, p. 89 – JHA Directive>; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC <OJ L 119 of 4 May 2016 – General Data Protection Regulation – GDPR>).

Irrespective of whether these EU legal acts are applicable to the powers of the Bavarian *Land* Office for the Protection of the Constitution (cf. Art. 4(2) third sentence of the Treaty on European Union – TEU), the competence to review the compatibility of these provisions with the fundamental rights of the Basic Law lies with the Federal Constitutional Court, and the constitutional complaint is admissible in this respect since the provisions do not implement binding EU law (cf. BVerfGE 155, 119 <162 ff. para. 83 ff.> with further references - Subscriber data II; 156, 11 <35 ff. para. 63 ff.> - Counter-Terrorism Database Act II; see also BVerfGE 152, 152 <168 f. para. 39, 42> - Right to be forgotten I; Federal Constitutional Court, Order of the Second Senate of 27 April 2021 - 2 BvR 206/14 -, para. 45 - Ecotoxicity). EU law does not contain any provisions that require, let alone lay down exhaustive rules on, the powers of a domestic intelligence service at issue here. 143

IV. Outcome of the admissibility assessment

Insofar as the constitutional complaint is directed at surveillance powers, it is partly admissible and partly inadmissible. The objection to Art. 9(1) first sentence BayVSG [*surveillance of private homes*] is admissible, as is the objection to the inadequate protection afforded to the core of private life under Art. 8a(1) first sentence no. 1, second to fifth sentence BayVSG. The objection to Art. 10(1) BayVSG [*remote searches of information technology systems*] is admissible insofar as the complainants challenge the statutory prerequisites for interference with fundamental rights, including interference with the core of private life, but is inadmissible insofar as they claim a violation of the objective guarantees arising from the fundamental right to protection of the confidentiality and integrity of information technology systems. The challenge to Art. 12(1) BayVSG [*tracking of mobile devices*] is admissible. The objection to Art. 15(2) BayVSG [*information requested from service providers*] is inadmissible, but the objection to Art. 15(3) BayVSG [*disclosure of traffic data originating from data retention*] is admissible. The challenge to Art. 16 BayVSG [*further information requests*] is inadmissible. The objections to Art. 18(1) [*undercover officers*], Art. 19(1) [*informants*] and Art. 19a(1) BayVSG [*observation outside the home*] are admissible. 144

Insofar as the constitutional complaint is directed at data processing and sharing powers, it is likewise partly admissible and party inadmissible. The challenge to Art. 25(1) no. 1 BayVSG is admissible to the extent that the provision permits the sharing of data for public security purposes. Likewise, it is admissible for the complainants to challenge the powers set out in Art. 25(1) no. 3 BayVSG permitting data to be shared for the purpose of performing other tasks within the recipient's remit. The objection to the sharing of data with bodies in other European states authorised under Art. 25(1a) BayVSG is only admissible to the extent that it concerns the sharing of data with public bodies. The challenge to Art. 25(2) BayVSG (data sharing with public prosecution offices, police authorities and other specialised authorities) is admissible insofar as it is directed at the data sharing powers under Art. 25(2) first sentence no. 2 BayVSG for the purpose of prosecuting, preventing and deterring considerable criminal offences, and insofar as it is directed at the data sharing powers under Art. 25(2) first sentence no. 3 BayVSG. However, the objection to the data sharing obligation under Art. 25(2) second sentence BayVSG is inadmissible. The challenge to the provision in Art. 25(3) first sentence no. 2 BayVSG authorising the sharing of data with foreign public bodies, supranational bodies and international bodies is admissible. The challenge to the powers conferred under Art. 25(3) first sentence no. 3 BayVSG to share information with non-public bodies is inadmissible. The objections to Art. 8b(2) first sentence no. 2 BayVSG and Art. 8b(3) BayVSG are admissible. 145

Finally, the challenges regarding the provisions on transparency and oversight provided for in the Bavarian Protection of the Constitution Act are in part insufficiently substantiated, and the relevant issues were in part insufficiently addressed in proceedings before the ordinary courts; this concerns the objection to Art. 11(2) third sentence, Art. 17(2) first sentence, Art. 20(1) and Art. 23(1) first sentence and third sentence nos. 1 and 2 BayVSG. 146

C. Merits

Insofar as the constitutional complaint is admissible, it is for the most part well-founded. The challenged provisions authorise the Bavarian *Land* Office for the Protection of the Constitution to covertly collect and to share personal data for the purpose of protecting the constitutional order. The provisions give rise to interferences with the fundamental rights under Art. 2(1) in conjunction with Art. 1(1) GG (general right of personality), Art. 10(1) GG (privacy of correspondence, post and telecommunications) and Art. 13(1) GG (inviolability of the home). The general right of personality is affected partly in its manifestation as a right to informational self-determination, partly in its manifestation as a right to protection of the confidentiality and integrity of information technology systems. The individual provisions at issue serve a legitimate purpose and satisfy the proportionality requirements with regard to their suitability and necessity; beyond that, however, the Constitution gives rise to overarching standards especially with regard to proportionality in the strict sense (see I. below), which these provisions largely fail to satisfy (see II. below). 147

I. General standards of substantive constitutionality

148 The constitutionality of the challenged surveillance powers depends on the fundamental right affected in each case and, above all, on the requirements derived from the principle of proportionality (see 1. below). Surveillance conducted by a domestic intelligence service interferes with fundamental rights in different ways than surveillance conducted by a police authority, and such interference may therefore be subject to modified proportionality requirements (see 2. below). The principle of proportionality in the strict sense gives rise to special requirements regarding the design of the legal framework in the field of domestic intelligence. These special requirements apply to provisions that confer data collection powers (see 3. below) and that confer powers authorising the further use and sharing of information (see 4. below). Additional constitutional requirements arise from the principle of legal clarity and specificity (see 5. below), from the fundamental rights protection afforded to the core area of private life (see 6. below), and due to the combined effect of different surveillance measures (see 7. below). Furthermore, special procedural safeguards are necessary to ensure that any interferences with fundamental rights are proportionate (see 8. below).

1. Principle of proportionality as central standard of review

149 In order to adhere to the constitutional principle of proportionality, measures carried out by domestic intelligence services must serve a legitimate purpose and be suitable, necessary and proportionate in the strict sense for achieving that purpose (cf. BVerfGE 67, 157 <173>; 120, 378 <427>; 154, 152 <239 f. para. 93>; established case-law).

150 a) The challenged provisions serve a legitimate purpose. The powers conferred thereunder are designed to enable the Bavarian *Land* Office for the Protection of the Constitution to perform its task of protecting the free democratic basic order, the existence of the Federation and of the *Länder*, and certain interests of the Federal Republic of Germany that concern its international relations (cf. Art. 3 BayVSG in conjunction with § 3 of the Federal Protection of the Constitution Act, *Bundesverfassungsschutzgesetz* – BVerfSchG). These are legal interests of significant constitutional weight (cf. BVerfGE 141, 220 <267 f. para. 100>). Since the Basic Law is committed to the principle of a militant democracy (cf. Art. 9(2), Art. 18, Art. 21 GG), restrictions of freedoms may be legitimate for the purpose of protecting the free democratic basic order. Persons with anti-constitutional aims should not be allowed to invoke the freedoms guaranteed by the Basic Law in order to endanger, undermine or destroy the constitutional order or the very existence of the state (BVerfGE 134, 141 <179 f. para. 112>; cf. also BVerfGE 30, 1 <29 ff.>; 149, 160 <194 para. 101>; established case-law). The Basic Law expressly permits the gathering of intelligence for the purpose of protecting the constitutional order: it sets out the legislative competence to do so and provides for the creation of bodies to carry out the relevant tasks (Art. 73(1) no. 10(b) in conjunction with Art. 70(1), Art. 87(1) second sentence

GG) (cf. BVerfGE 134, 141 <180 para. 113>). The Basic Law does this in recognition of the fact that endeavours and activities directed against the constitutional order or the security and existence of the state are also carried out by groups conspiring against the state, and that the domestic intelligence services can therefore only perform their tasks effectively if they can use covert intelligence service methods (cf. BVerfGE 146, 1 <50 para. 110>; 156, 270 <304 para. 104>). In doing so, the Basic Law accepts – sometimes explicitly – that certain restrictions to transparency and judicial protection will then be necessary, which will have to be compensated in other ways (cf. Art. 10(2) second sentence, Art. 19(4) third sentence GG), even though transparency and judicial protection are two particularly important aspects of the rule of law.

b) There is no doubt that the challenged powers are in principle suitable and necessary under constitutional law for achieving these purposes. 151

c) In terms of their statutory design, the powers of the domestic intelligence services are subject to differentiated requirements arising from the principle of proportionality in the strict sense. How stringent these requirements are in each case depends on the severity of interference resulting from the measure in question (cf. BVerfGE 141, 220 <269 para. 105>; 155, 119 <178 para. 128>) and the particular fundamental right at issue. In recent decisions, the Federal Constitutional Court has summarised these requirements in relation to the covert surveillance measures carried out by police authorities (cf. BVerfGE 141, 220 <268 ff. para. 103 ff.>; 155, 119 <186 ff. para. 145 ff.>). This is also the starting point for assessing the powers of the domestic intelligence services, both with regard to the requirements that apply to data collection and with regard to the requirements that apply to the further use and sharing of that data (cf. also BVerfGE 154, 152 <239 para. 141>). However, these requirements must be further specified and to some extent modified in light of the special tasks performed by domestic intelligence services and the particular weight of interference resulting from the measures they carry out (cf. BVerfGE 100, 313 <383>; 120, 274 <330>; 125, 260 <331>; 130, 151 <206>; 156, 11 <56 para. 119>). 152

2. Particularities of intelligence service powers as opposed to police powers

To some extent, the principle of proportionality in the strict sense gives rise to different requirements for the design of surveillance powers depending on whether those powers are conferred upon a domestic intelligence service or a police authority. The fact that, under the currently applicable legal framework, domestic intelligence services have specific surveillance and intelligence gathering responsibilities and do not have the operational follow-up powers that police authorities do – which would allow them to take direct operational action based on the intelligence obtained from a surveillance measure (see a) below) – can justify linking the use of their surveillance powers to modified thresholds (see b) below). However, strict requirements must then be applied to the sharing of information with other authorities (see c) below). 153

a) Like intelligence services in general, domestic intelligence services differ from 154

police authorities in that, under the currently applicable legal framework, they do not have responsibility for operational activities (cf. BVerfGE 133, 277 <324 ff. para. 115 ff.> for extensive details). The task of police and prosecution authorities to prevent, avert and prosecute criminal offences and to avert other dangers to public security and order is characterised by operational responsibility and the power to enforce certain measures against individuals, if necessary by force (cf. BVerfGE 156, 11 <51 para. 102> with further references). Domestic intelligence services, on the other hand, are tasked with the precautionary investigation of threat situations before any actual dangers arise. They are called upon to keep general track of the potential threat posed by a wide range of different endeavours, monitoring such activities even without the presence of any specific danger (BVerfGE 133, 277 <325 para. 116>). This is reflected in a restriction of their powers: they do not have police powers, nor may they request – by way of inter-agency administrative assistance (*Amtshilfe*) – that the police carry out measures for which they themselves have no authorisation (BVerfGE 133, 277 <326 f. para. 119>). Domestic intelligence services thus have no coercive police powers at their disposal that would enable them to enforce specific public security or prosecution measures against individuals by force, based on information they have previously obtained from surveillance.

b) These differences have implications for the constitutional requirements that apply to the data collection powers of domestic intelligence services (see para. 174 ff. below for specific details; on the implications for the requirements applicable to the sharing of information thereby obtained, see para. 170 ff. below and for specific details see para. 225 ff. below). 155

aa) In principle, the fact that domestic intelligence services do not have their own operational follow-up powers justifies linking the data collection powers conferred upon them for their surveillance tasks to modified versions of the thresholds applicable to police authorities. This is due to the lower severity of the resulting interference and also reflects the special nature of the tasks carried out by the domestic intelligence services. 156

(1) Generally speaking, the severity of interference with fundamental rights resulting from a surveillance measure partly depends on the potential uses of the obtained data (cf. BVerfGE 65, 1 <45 f.>; 155, 119 <178 f. para. 129>); i.e. it also depends on what disadvantages the holders of fundamental rights might face, or have reason to fear, from the further use of the data (cf. BVerfGE 100, 313 <376>; 107, 299 <320>; 109, 279 <353>; 113, 348 <382>; 115, 320 <347 f.>; 118, 168 <197>; 120, 378 <403>). This point is reflected in the constitutional requirements that apply to the thresholds for interference applicable to actions by public authorities. 157

When it comes to the police, their powers to carry out covert surveillance measures are subject to strict conditions. Since the tasks performed by the police are characterised by operational responsibility and the power to enforce certain measures against individuals, if necessary by force, such powers must be narrowly and precise- 158

ly defined (cf. BVerfGE 156, 11 <51 para. 102> with further references). In the area of public security measures, the collection of data by means of covert surveillance – an activity which entails highly intrusive interferences – is generally only proportionate if there is a sufficiently specific and foreseeable danger to particularly weighty legal interests in the individual case and if the person targeted by these measures appears, from the perspective of a reasonable observer examining the objective circumstances, to be involved therein (cf. BVerfGE 141, 220 <271 para. 108 f.>). The term “specific danger” (*konkrete Gefahr*), as traditionally used in police law, accordingly requires a situation where it can be assumed with sufficient probability that the chain of events that is objectively to be expected would lead, in the individual case and within the foreseeable future, to the violation of a legal interest protected under public security law if the situation were to unfold without intervention (cf. BVerfGE 141, 220 <271 para. 111> with further references). It is true that a sufficiently identifiable danger (*hinreichend konkretisierte Gefahr*) can exist even before the causal chain leading to the damage is foreseeable with sufficient probability, provided that there are already specific facts indicating an impending danger (*drohende Gefahr*) to an exceptionally significant legal interest in the individual case. But even then, it must at least be possible to determine, based on these facts, the type of incident that might occur, and that it will occur within a foreseeable timeframe. Furthermore, the facts must indicate the involvement of specific persons whose identity is known at least to such an extent that the surveillance measures can be targeted at them and for the most part limited to them (cf. BVerfGE 141, 220 <272 f. para. 112> for further details).

When surveillance measures are carried out by a domestic intelligence service, however, the severity of the resulting interference is generally lower because domestic intelligence services do not have their own operational follow-up powers. This can justify linking the use of their surveillance powers to modified thresholds (cf. BVerfGE 130, 151 <206>; 133, 277 <325 ff. para. 117 ff.>; 154, 152 <242 para. 149>; 156, 11 <51 para. 103 f.>; […]). 159

(2) Even so, the surveillance measures of a domestic intelligence service still have to be linked to certain prerequisites in order to ensure that the resulting interferences with fundamental rights are proportionate when measured in terms of their severity and the purpose pursued. Interferences with fundamental rights must be justified by sufficient grounds – i.e. the so-called threshold for interference must be reached – and the interference must serve to protect legal interests of sufficient weight (cf. BVerfGE 150, 244 <280 f. para. 90>; established case-law). These are essential core requirements arising from the rule of law and they apply to all state action. They are generally also applicable to intelligence services such as Offices for the Protection of the Constitution (*Verfassungsschutz*), i.e. the domestic intelligence services (cf. BVerfGE 154, 152 <244 f. para. 155 f.>). 160

The Federal Constitutional Court’s judgment on the strategic surveillance of foreign telecommunications by the Federal Intelligence Service (*Bundesnachrichtendienst*) does not merit a different conclusion. It is true that the particularly intrusive powers at 161

issue in that case were found to be in principle justifiable under constitutional law even though the legislator had exempted the Federal Intelligence Service from having to observe any specified thresholds in that regard and had not limited the powers in question by linking their use to specific and objectively determined grounds (cf. BVerfGE 154, 152 <240 para. 143, 244 f. para. 154 f.>). However, this cannot be interpreted as meaning that intelligence services are generally exempt from having to observe specified thresholds for the exercise of their powers (cf. also BVerfGE 100, 313 <389 f.>). In the case of strategic foreign surveillance, the threat posed by operational follow-up measures is specifically lessened by the fact that foreign surveillance concerns activities in other countries, where the German state is not vested with sovereign powers (cf. BVerfGE 154, 152 <242 para. 149, 248 f. para. 165>). Furthermore, the surveillance of occurrences in other states takes place under special conditions because the German state generally has no or very few resources for gathering intelligence and is not vested with sovereign powers granting it direct access to information (cf. BVerfGE 154, 152 <246 para. 159>). This is what justifies the lack of any specific thresholds for interference in that particular context. For other surveillance measures, reliable thresholds are still necessary in accordance with the general requirements (cf. BVerfGE 154, 152 <245 para. 156>).

(3) Although the surveillance powers of the domestic intelligence services have to be linked to specified thresholds, it may nonetheless be permissible to use modified versions of the thresholds applicable to police surveillance due to the generally lower severity of the resulting interference (see para. 156 ff. above). By modifying the thresholds, the legislator can take account of the nature of the activities performed by the domestic intelligence services and the special responsibility they bear for carrying out the precautionary investigation of anti-constitutional endeavours before specific dangers arise (cf. BVerfGE 120, 274 <330>). 162

Setting a generally applicable threshold requiring the presence of danger in the sense used for police action would fail to take account of the specific range of tasks carried out by the domestic intelligence services ([...]). The police are only authorised to carry out covert surveillance measures if circumstances representing a danger to public security are already sufficiently identifiable (see para. 158 above), whereas in order for the domestic intelligence services to carry out their tasks, they need to have powers that can be exercised independently of any such specific circumstances. Surveillance activities of the domestic intelligence services are aimed at enabling the state to detect the emergence of potential threats to the protected elements of the constitutional order even before a specific danger arises. An example of this would be where several persons work towards undermining these protected elements by collaborating in a coordinated and organised manner; in this case, the threat to constitutional principles warranting surveillance lies in an organised structure pursuing anti-constitutional ideas ([...]). At the same time, potential threats are no longer viewed as stemming purely from activities that involve a degree of organisation, but are now seen as also emanating from certain narratives on social media which, al- 163

though ostensibly independent, share similar goals and feed into related initiatives due in part to the mutually reinforcing dynamic of communication in social networks ([...]). In both cases, a threat situation warranting surveillance can arise even without the existence of an identifiable danger (*konkretisierte Gefahr*) in the sense used for police action.

The requirement that a surveillance measure by a domestic intelligence service be necessary in the individual case to investigate a specific activity or group warranting surveillance is thus generally equivalent in constitutional terms to the requirement that police measures only be carried out if an identifiable danger is present (cf. BVerfGE 155, 119 <189 para. 151, 202 para. 179 at the end>). Nonetheless, a heightened need for surveillance may be required in certain circumstances, depending on the severity of interference resulting from the surveillance measure in question (for more on this point, see para. 190 ff. below). 164

bb) However, not all covert surveillance measures carried out by the domestic intelligence services may be authorised on the basis of such modified prerequisites. 165

(1) If the interference resulting from a surveillance measure by a domestic intelligence service already constitutes such a severe impairment of fundamental rights on its own – i.e. even before any possible follow-up interferences are taken into consideration – that it is irrelevant whether any subsequent interferences may arise from the further use of the obtained information, the same requirements as for police measures must be applied. This is the case if the information obtained from a surveillance measure is especially comprehensive and could lead to extensive insight being gained into one's personality, as for example can occur with remote searches of information technology systems (cf. BVerfGE 120, 274 <331>). In such cases, the fact that the domestic intelligence services are limited to the gathering of precautionary intelligence – i.e. the fact that they lack operational follow-up powers (see para. 154 above) – is no longer sufficient to justify deviating from the prerequisites for interference derived from the principle of proportionality (cf. BVerfGE 120, 274 <329 f.>). 166

This must be distinguished from the requirements for protecting the core of private life (see para. 275 ff. below). Safeguards to protect the core of private life are necessary not only in the case of measures that enable particularly extensive insight to be gained into one's personality, but also in respect of other measures that typically intrude deeply into the private sphere and are able to record highly confidential situations with significant probability (cf. BVerfGE 141, 220 <295 para. 176>). Safeguards to protect the core of private life must be provided for; in respect of intelligence service action, too, providing for such safeguards is possible and indeed constitutionally necessary (see para. 275 below). 167

(2) (a) In the case of remote searches of information technology systems, domestic intelligence services are subject to the same requirements as police authorities because remote searches entail the risk of the affected individual's personality being extensively spied upon by the state (cf. BVerfGE 120, 274 <331>). With regard to re- 168

mote searches, the constitutional requirements that apply to the factual grounds justifying such measures do not vary. Since the impairment of fundamental rights resulting from the interference is always the same for affected persons, there is no need to differentiate between police authorities and domestic intelligence services in this case. For the purposes of weighing remote searches, it is in principle irrelevant that the police and domestic intelligence services have different responsibilities and powers, and that, in consequence, the depth of interference resulting from their measures may differ (cf. BVerfGE 120, 274 <329 ff.>).

(b) The same applies to the acoustic or visual surveillance of private homes by a domestic intelligence service, as already follows from Art. 13(4) GG. Pursuant to that provision, domestic intelligence services are permitted to carry out the preventive surveillance of private homes only for the purpose of averting an acute danger (*dringende Gefahr*) to public safety, especially a danger to life or to the general public (cf. BVerfGE 109, 279 <378 f.>; 130, 1 <32>; 141, 220 <271 para. 110, 296 para. 184>). In this respect, the term “acute danger” qualifies both the extent of possible damage to the legal interests the measure aims to protect and the probability that the damage will occur (cf. BVerfGE 141, 220 <271 para. 111> with further references). Art. 13(4) GG formulates these particularly stringent requirements without distinguishing between the different types of authority carrying out the measure. Domestic intelligence services are not exempted ([...]). There is nothing in the text of the Basic Law to indicate that distinctions are to be made based on the type of authority involved ([...]). This is consistent with the special nature of the interference. Surveillance of a private home enables the authority carrying out the measure to gain direct acoustic and visual access to every action or omission and every movement of the person under surveillance within their own private space. The affected person is directly and comprehensively exposed to the authority’s observation. Given the particular expectations of confidentiality that are legitimately associated with the home, individuals under surveillance in a home environment are at especially high risk of unknowingly and unintentionally providing deep and wide-ranging insights into their personality (cf. BVerfGE 109, 279 <313 f.>; 141, 220 <295 f. para. 180>). 169

c) In cases other than remote searches and surveillance of private homes, it is only constitutionally permissible to link the covert surveillance measures of a domestic intelligence service to modified thresholds if any sharing of the obtained information with other bodies is subject to the same constitutional requirements that would apply to the receiving bodies if they were to carry out equivalent interferences with fundamental rights by collecting the information themselves (“criterion of a hypothetical recollection of the data”; cf. BVerfGE 141, 220 <327 f. para. 287>; further details under para. 230 ff. below). 170

The granting of extensive surveillance powers to domestic intelligence services is only justifiable under constitutional law if hurdles are in place to prevent the obtained information from being shared unconditionally with other authorities that have operational follow-up powers (principle of separation of police and intelligence data – *infor-* 171

mationelles Trennungsprinzip, cf. BVerfGE 133, 277 <329 para. 123>; 156, 11 <50 para. 101, 51 f. para. 105>). If these hurdles were not there, the fact that domestic intelligence services lack their own operational follow-up powers would not ultimately offer any protection to persons under surveillance: the intrusive follow-up measures that are unavailable to domestic intelligence services could then be carried out by authorities with operational powers, which would be able to utilise the information obtained by the domestic intelligence services without having to satisfy the data collection requirements that apply to them as operational authorities. For the receiving authorities, this would circumvent the thresholds that apply to authorities with operational powers so as to protect fundamental rights; for the domestic intelligence services, the fact that they do not have operational follow-up powers would lose its protective function.

172 In order to prevent either of these from happening, it is essential under constitutional law to ensure that sufficient data sharing requirements are in place. Without this second hurdle, it would be necessary to subject domestic intelligence services and police authorities to the same thresholds for the exercise of their surveillance powers. In its Data Retention judgment, the Federal Constitutional Court took the position that the thresholds should be identical regardless of whether the surveillance is carried out by an intelligence service or a police authority. This again was aimed at preventing the strict constitutional requirements applicable to police surveillance powers from being undermined – something that would occur if data obtained by an intelligence service were to be utilised by a police authority prior to the emergence of any danger, despite the police authority not itself being permitted to conduct surveillance of this nature under such conditions. In order to prevent the law from being circumvented in this manner, it appeared necessary to link the powers of both authorities to the same requirements (cf. BVerfGE 125, 260 <331 f.>).

173 The surveillance powers of the intelligence services do not, however, have to be linked to the strict hurdles applicable to police authorities if the obtained information is shared in ways that satisfy the criterion of a hypothetical recollection of the data – a criterion which has since been further developed. According to this criterion, if a public security authority wishes to make further use of data collected by an intelligence service, such further use must satisfy the same requirements concerning the legal interest to be protected and the so-called threshold for data sharing (cf. BVerfGE 154, 152 <268 para. 220>; 156, 11 <55 para. 115>) as would apply if the shared data were to be collected again by the receiving authority itself (see para. 231 below for more details). Together, these requirements concerning the legal interest and the applicable thresholds are designed to prevent the prerequisites for interference from being undermined. As such, they serve to protect the fundamental rights of affected persons. Thus, if the legislator provides for sufficiently robust data sharing requirements, it is not necessary for all the surveillance powers of the domestic intelligence services to be linked to the same requirements as for police surveillance powers simply to ensure that the possibilities for the further use of data are adequately taken into

account. At the same time, linking the data collection measures of the domestic intelligence services to modified versions of the thresholds applicable to police action is only justifiable if sufficient data sharing requirements have been put in place (see para. 235 ff. below for further details).

3. Proportionality (in the strict sense) of data collection

The covert surveillance powers of the domestic intelligence services are subject to proportionality requirements, the strictness of which depends on the severity of interference with fundamental rights in each case (cf. BVerfGE 141, 220 <269 para. 105>; 155, 119 <178 para. 128>). In this respect, constitutional requirements exist with regard to the legal interest to be protected by the surveillance and the so-called threshold for interference, i.e. the grounds for the surveillance (cf. BVerfGE 141, 220 <269 para. 104, 270 f. para. 106 ff., 271 ff. para. 109 ff.>). However, given that surveillance measures of the domestic intelligence services always serve to protect particularly high-ranking legal interests (see para. 150 above), the only question at issue here is whether the thresholds for interference set out in the Bavarian Protection of the Constitution Act are proportionate. Covert surveillance measures that could lead to particularly extensive insight being gained into one's personality and that are therefore subject to the same proportionality requirements as police surveillance require the presence of at least an identifiable danger (see a) below). For other covert surveillance measures, there must be a need for surveillance specifically relating to the protection of the constitutional order (see b) below). 174

a) aa) In the case of measures by a domestic intelligence service that could lead to particularly extensive insight being gained into one's personality (see para. 165 ff. above), the principle of proportionality in the strict sense imposes the same requirements on the thresholds for interference as it does for police surveillance. 175

(1) With remote searches of information technology systems, data collection is only proportionate if at least an identifiable danger is present, i.e. if certain facts make it at least possible to determine the type of incident that might occur, and that it will occur within a foreseeable timeframe, and if these facts furthermore indicate the involvement of specific persons whose identity is known at least to such an extent that the surveillance measure can be targeted at and for the most part limited to them (cf. BVerfGE 141, 220 <272 f. para. 112> for further details; in this respect also BVerfGE 120, 274 <328 f.>). 176

(2) With surveillance of private homes, the threshold follows from Art. 13(4) GG. This particularly deep intrusion into the private sphere is only permitted for the purpose of averting an acute danger. In order to satisfy the criterion of acute danger, strict requirements that go beyond the criterion of specific danger must be met (cf. BVerfGE 141, 220 <296 para. 184>). One such requirement concerns the probability that damage will occur (cf. BVerfGE 141, 220 <271 para. 110>). 177

bb) Insofar as a domestic intelligence service may not then be authorised to conduct 178

a measure for precautionary intelligence-gathering purposes but only for the purpose of averting at least an identifiable danger, the authorisation may furthermore only be granted on a subsidiary basis, i.e. only in the event that suitable police assistance for the legal interest at risk cannot otherwise be timely obtained (as set out in § 9(2) first sentence BVerfSchG).

This applies to remote searches and surveillance of private homes. Authorisation to carry out such measures may only be granted to a domestic intelligence service for the purpose of averting at least an identifiable danger or an acute danger respectively (see para. 168 f. above). Yet domestic intelligence services do not have operational capabilities that would generally enable them to avert danger on their own. It is true that the emergence of a specific danger does not mark the point at which domestic intelligence services are obliged to cease their operations. On the contrary, they are in principle allowed to continue their investigations beyond this point ([...]). But under normal circumstances, they would not be able to avert such danger on their own and would instead have to share the obtained information with a public security authority that has operational powers ([...]). However, this would usually exacerbate the fundamental rights impairment because the sharing of information with a public security authority constitutes a new and separate interference (cf. BVerfGE 154, 152 <266 para. 212> with further references). It expands the group of those who receive and can utilise the information, to the detriment of those affected by the surveillance (cf. BVerfGE 100, 313 <367>). 179

In order to avoid unnecessary interferences with fundamental rights, information-gathering measures which from the outset may only be authorised for the purpose of preparing to avert a specific danger must therefore, in principle, be carried out by the public security authority itself. Only if the measure cannot be carried out by a public security authority in a suitable or timely manner is it constitutionally permissible, as an exception, for remote searches or the surveillance of private homes to be conducted on a subsidiary basis by a domestic intelligence service ([...]). 180

b) Unless a surveillance measure already constitutes an interference of such severity on its own that the possibility of other interferences arising from further uses of the obtained information is irrelevant (see para. 166 above), the surveillance powers of a domestic intelligence service do not have to be linked to the presence of a specific or identifiable danger in the same sense as for police action (see para. 158 above). However, in order for the measure to be proportionate in the strict sense, a sufficient need for surveillance specifically relating to the protection of the constitutional order is then required (see aa) below): the measure must be necessary in the individual case to investigate a specific activity or group that warrants surveillance by an intelligence service, and it must be based on sufficient factual indications (cf. BVerfGE 130, 151 <206>; 155, 119 <189 para. 151>; 156, 11 <56 para. 119>). The greater the severity of interference resulting from the surveillance measure, the more urgent this need for surveillance must be. The principle of proportionality furthermore gives rise to special requirements that apply when persons are affected by the surveillance who 181

are not themselves part of the endeavour at issue or otherwise acting in furtherance of the endeavour (see bb) below). Depending on the severity of interference resulting from the measure in question, the principle of proportionality in the strict sense can also make it necessary to subject the measure to *ex ante* oversight by an independent body (see cc) below).

aa) The threshold for the use of surveillance measures specifically relating to the protection of the constitutional order requires the presence of sufficient indications that a particular endeavour warrants surveillance (see (1) below) and that the measure is necessary in the individual case to investigate the endeavour (see (2) below). 182

(1) An endeavour may only be assumed to be directed against the protected elements of the constitutional order (see (a) below) if sufficient factual indications are present to support this assumption (see (b) below). The greater the severity of the interference, the more urgent the need for surveillance of the observed activity or group must be (see (c) below). 183

(a) Statutory definitions of the endeavours to be monitored by the domestic intelligence services can be found under § 4(1) BVerfSchG, to which Art. 4(1) BayVSG refers. According to these definitions, endeavours directed against the free democratic basic order are politically motivated, goal-oriented activities within or on behalf of a group of persons, aimed at eliminating or neutralising any of the constitutional principles listed as part of the free democratic basic order in § 4(2) BVerfSchG. Endeavours directed against the existence of the Federation or a *Land* are politically motivated, goal-oriented activities within or on behalf of a group of persons, aimed at eliminating the freedom from foreign rule of the Federation or a *Land*, destroying their internal unity or separating off part of their territory. Endeavours directed against the security of the Federation or a *Land* are politically motivated, goal-oriented activities within or on behalf of a group of persons, aimed at significantly impairing the proper functioning of the Federation, the *Länder* or their institutions. According to § 4(1) third and fourth sentence BVerfSchG, such endeavours can also be the work of an isolated individual if the relevant individual's activities are directed at achieving the aforementioned goals. 184

The Federal Administrative Court (*Bundesverwaltungsgericht*) has further specified how anti-constitutional endeavours within the meaning of § 4 BVerfSchG are to be understood. Anti-constitutional endeavours take an active but not necessarily belligerent or illegal approach towards achieving their goals. In order to be categorised as such, anti-constitutional endeavours must be objectively capable of having a political impact in the long or short term. Going beyond the mere holding of political opinions, anti-constitutional endeavours must be geared towards the achievement of a political goal, the aim of which must be to impair one of the elements of the free democratic basic order. The persons responsible must be actively working towards the successful achievement of that goal. Mere criticism of constitutional principles is not sufficient to warrant categorisation as an anti-constitutional endeavour, unless the 185

criticism is accompanied by a statement announcing or encouraging specific action to destroy said constitutional principles (cf. Federal Administrative Court, *Bundesverwaltungsgericht* – BVerwG, Judgment of 14 December 2020 - 6 C 11/18 -, juris, para. 20, with further references). Although the Federal Administrative Court's interpretation only explicitly deals with endeavours directed against the free democratic basic order, its structural similarity to the legal definitions in § 4(1) first sentence BVerfSchG means that it can also be applied to endeavours directed against the other protected elements of the constitutional order ([...]).

Using this interpretation of anti-constitutional endeavours as a framework to determine the basic threshold at which the domestic intelligence services may carry out surveillance using intelligence service methods does not raise any constitutional concerns (cf. on the insignificance of merely criticising constitutional values and principles, BVerfGE 113, 63 <81 f.>; 149, 160 <197 f. para. 108>). Nor is it constitutionally objectionable in principle if the domestic intelligence services are granted powers to use intelligence service methods to obtain information on groups that threaten the protected elements of the constitutional order without actually breaking the law. This reflects the special responsibility of the domestic intelligence services for carrying out precautionary investigations of anti-constitutional endeavours before specific dangers arise (BVerfGE 120, 274 <330>). Nor do the surveillance measures of the domestic intelligence services have to be limited from the outset to militant endeavours or endeavours involving incitement to hatred (cf. BVerfGE 120, 274 <349>), and they may be justifiable before an endeavour assumes an outwardly active and belligerent stance towards the fundamental principles of the Constitution (cf. on the requirements for prohibiting an association, BVerfGE 149, 160 <197 f. para. 108>). However, depending on the severity of interference, the need for surveillance may in some cases have to satisfy more demanding constitutional requirements (see para. 190 ff. below). 186

(b) Sufficient factual indications that an endeavour is threatening the protected elements of the constitutional order are required (cf. BVerfGE 120, 274 <349>; see also BVerfGE 156, 11 <56 para. 119>; on the inclusion of a group in an annual report on the protection of the Constitution, see BVerfGE 113, 63 <81>). Vague suspicions that a certain group might be directed against the free democratic basic order are not sufficient (cf. BVerfGE 120, 274 <349>). 187

In § 4(1) fifth sentence BVerfSchG, the federal legislator has set the explicit condition that a domestic intelligence service may only collect and evaluate information, i.e. may only engage in the surveillance of an endeavour ([...]), on the basis of factual indications. According to the case-law of the administrative courts, this does not require absolute certainty that an anti-constitutional endeavour actually exists, nor does it require the presence of danger within the meaning of police law. However, mere supposition, speculation and conjecture with no foundation in observable fact is insufficient. The required indications must be in the form of concrete and sufficiently tangible circumstances that are capable of establishing a suspicion that an anti-constitutional endeavour exists. Surveillance may only be authorised on the basis of facts 188

that were known to the domestic intelligence service at the time when the surveillance measure in question began. Based on the factual indications known to it, the domestic intelligence service must draw up a prognosis as to whether the suspicion is likely to be well-founded. The domestic intelligence service is not therefore permitted to engage in surveillance irrespective of whether any suspicion exists, i.e. it is not allowed to conduct surveillance on a purely speculative basis with the aim of establishing a suspicion in the first place or of generating and retaining data for subsequent use (cf. most recently BVerwG, Judgment of 14 December 2020 - 6 C 11/18 -, juris, para. 23 ff. with further references).

189 Thus, while the permissibility of a surveillance measure does not necessarily depend upon an endeavour having been proven to exist, indications are nonetheless required in the form of concrete and sufficiently tangible circumstances that are capable of establishing a suspicion that an anti-constitutional endeavour exists. Prior to any systematic surveillance being carried out, indications of this nature can primarily be obtained from generally available sources of information ([...]). Here again, there are no constitutional objections to using this framework to determine the basic threshold at which a domestic intelligence service may carry out surveillance measures using intelligence service methods. However, depending on the severity of interference resulting from the surveillance measure, the factual substance of this threshold may in some cases have to satisfy more demanding constitutional requirements (see para. 192 ff. below).

190 (c) The greater the severity of the interference (see (aa) below), the more urgent the need for surveillance of the observed activity or group must be (see (bb) below). The legislator must set forth in a sufficiently specific and clear manner what level of need for surveillance is required in each case (see (cc) below).

191 (aa) The covert surveillance measures of the domestic intelligence services can give rise to very severe interferences with fundamental rights. This applies not just to measures which in themselves already enable particularly extensive insight to be gained into one’s personality, such as remote searches and surveillance of private homes, but also to measures that are less intrusive when carried out by a domestic intelligence service than when carried out by a police authority. Here too, the severity of interference resulting from surveillance by a domestic intelligence service depends in particular on the extent of the possible insight into one’s personality, on whether especially private information can be obtained, and on whether legitimate expectations of confidentiality are breached (cf. BVerfGE 141, 220 <269 para. 105>; 155, 119 <229 para. 253>). From this perspective, measures such as long-term observation (especially involving the recording of images), the surveillance of non-public conversations, and the use of informants and undercover officers give rise to particularly severe interferences (cf. BVerfGE 141, 220 <294 para. 174>). The severity of the interference is also affected by the duration of a surveillance measure (cf. BVerfGE 141, 220 <293 para. 171>).

(bb) The severity of the interference with fundamental rights must be balanced against the need for surveillance of the (putative) endeavour. This primarily depends on the seriousness of the threat to the protected elements of the constitutional order. Various indications may be used as a basis for assessing the urgency of the need for surveillance, but they must always be related in some way to these protected elements (Art. 73(1) no. 10(b) GG; see also § 3(1) BVerfSchG and Art. 3 BayVSG). 192

The need for surveillance becomes more urgent as the factual indications make it appear increasingly possible that the protected elements of the constitutional order are at specific risk and that actions directed against them may succeed (cf. BVerfGE 113, 63 <81 f.>; 120, 274 <348>; cf. with regard to Art. 21(2) GG, BVerfGE 144, 20 <224 f. para. 585> - Prohibition proceedings concerning the political party NPD; “potentiality”). In assessing whether an endeavour warrants a heightened need for surveillance, criteria that indicate whether the endeavour is “seeking” to achieve its aims within the meaning of Art. 21(2) GG (prohibition of unconstitutional parties) may be applied accordingly (cf. BVerfGE 144, 2 <224 ff. para. 585 ff.>; cf. on the lower standard under Art. 9(2) GG [regarding the prohibition of associations] requiring that the endeavour be “directed against” the constitutional order, taking an “actively belligerent stance”, BVerfGE 149, 160 <197 ff. para. 108 f.>). 193

For example, a heightened need for surveillance may be warranted by the fact that an endeavour is directed at the use of violence, or at preparing to use violence, or that it engages in incitement to hatred (cf. BVerfGE 120, 274 <349>; 144, 20 <223 para. 580>; see also § 9a(1) last part of second sentence BVerfSchG; […]). The use of violence also indicates a certain potentiality with regard to the aims pursued by the endeavour (cf. BVerfGE 144, 20 <226 para. 588>). 194

The size and social influence of an endeavour can be further indications (cf. *Bundestag* document, *Bundestagsdrucksache* – BTDrucks 18/4654, p. 26; […] cf. also BVerfGE 144, 20 <224 para. 583>: “the more established they become” […]). This can take into account the situation of the endeavour (number of members and sympathisers and whether those numbers are rising or falling, organisational structure, degree of mobilisation, ability to campaign, financial situation), the endeavour’s impact in society (publications, alliances, supporter structures) and its representation in public office and representative bodies, from which it can be inferred whether it appears possible that the aims pursued by the endeavour will be realised. A heightened need for surveillance requires that there are sufficient specific and weighty indications suggesting that the actions of the endeavour against the protected elements of the constitutional order may succeed. This can take account both of the prospects for the endeavour’s success in merely participating in the political debate and also of the possibility that the endeavour’s political aims will be successfully achieved by other means (cf. accordingly with regard to Art. 21(2) GG, BVerfGE 144, 20 <225 f. para. 587>). 195

Another factor capable of influencing the need for surveillance is the degree of se- 196

crecy surrounding an endeavour (cf. BTDrucks 18/4654, p. 26; […]). If views are openly expressed or readily accessible in the public domain, there is less justification for conducting particularly intrusive surveillance than if ideas are only shared in closed communication groups ([...]).

If an endeavour operates entirely within the law, it is likewise harder to justify a heightened need for surveillance that would permit the use of intrusive methods ([...]). In certain (exceptional) cases, however, a lawful endeavour may warrant a heightened need for surveillance. Ultimately, this depends on the specific circumstances of the individual endeavour (cf. BVerfGE 144, 20 <221 f. para. 578>). It is not impossible for an endeavour operating below the threshold of criminal conduct to acquire a degree of potentiality by disseminating highly effective misinformation on a massive scale, for example, or by creating an atmosphere of fear and intimidation which would be capable in the long term of undermining the free process of forming the political will, thereby effectively subverting that process with the goal of eliminating the free democratic basic order (cf. BVerfGE 144, 20 <226 para. 588> on Art. 21(2) GG). A particular need for surveillance can also arise if an endeavour is directed at the commission of particularly serious criminal acts (cf. for example Art. 19(2) third sentence BayVSG with reference to § 3(1) of the Article 10 Act, *Artikel 10-Gesetz* – G 10 and § 100b(2) of the Code of Criminal Procedure, *Strafprozessordnung* – StPO). 197

The need for surveillance may conversely become less urgent, the longer a surveillance measure continues without producing any factual indications as to whether, or to what extent, an endeavour (still) poses a specific risk to the protected elements of the constitutional order and whether the actions directed against these protected elements could succeed (cf. also BVerwG, Judgment of 7 December 1999 - 1 C 30/97 -, juris, para. 34, Decisions of the Federal Administrative Court, *Entscheidungen des Bundesverwaltungsgerichts* – BVerwGE 110, 126 <137 f.>; […]). 198

(cc) The legislator must, in a sufficiently specific and clear manner, define thresholds corresponding to the severity of interference resulting from the different surveillance powers. In doing so, it must set forth what level of need for surveillance is required in each case. 199

(α) The actions of the domestic intelligence services are subject to substantive requirements that arise from the principle of proportionality and thus from the Constitution itself. Nevertheless, the legislator may not leave the task of specifying these proportionality requirements entirely to the administrative authorities. Statutory provisions authorising the covert collection and processing of data are subject to particularly stringent requirements (cf. BVerfGE 113, 348 <375 ff.>; 120, 378 <407 f.>; 141, 220 <265 para. 94>; 150, 244 <278 f. para. 82>) in terms of their specificity and clarity (cf. BVerfGE 156, 11 <45 f. para. 86 f.>). These requirements differ depending on the severity of interference in each case and are thus closely linked to the respective substantive requirements of proportionality (cf. BVerfGE 141, 220 <265 para. 94>). For covert measures capable of reaching deep into the private sphere, as 200

is the case with most of the surveillance powers at issue here, the specificity requirements are strict. This reflects the fact that protection can only be effectively guaranteed against state data collection and processing activities if the underlying legislative framework is sufficiently specific. Affected persons are not usually aware that they are being targeted by covert surveillance measures and are thus seldom able to take legal action to defend themselves. As a result, the contents of the relevant legislation can only be specified to a limited extent through the interplay of practical application and judicial review (cf. BVerfGE 141, 220 <265 para. 94>). It is true that some possibilities to gradually specify the legal framework involving aspects of independent oversight do exist under the law as it currently stands; the general data protection oversight exercised by the *Land* Data Protection Officer is one such avenue here. Given the limited possibilities for legal recourse, such oversight assumes particular importance for the protection of fundamental rights. But this is quite different than judicial review being available to affected persons in every individual case. In order to ensure that the authorities involved are properly bound by the law, the legislator must enact statutory provisions that are specific enough to be capable on their own of providing standards that direct and limit the actions of the administration (cf. BVerfGE 156, 11 <45 para. 86>).

Intelligence services, including domestic intelligence services, are not exempt from the specificity requirements. It is true that they must largely perform their tasks covertly. However, this does not mean that as little as possible should be known about their activities or that the relevant 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 their activities and the limits of their powers. 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. The requirement that the powers granted to the domestic intelligence services be clearly and specifically set out in law does not undermine the possibility of keeping the intelligence obtained through such powers secret. In themselves, the powers merely create abstract legal possibilities; they do not allow conclusions to be drawn about whether, how and to what extent a domestic intelligence service makes use of such powers and with what results (cf. BVerfGE 154, 152 <238 f. para. 138 ff.>). 201

(β) Thus, where covert surveillance powers are conferred upon the domestic intelligence services, the legislator itself must set forth, in a manner that satisfies the constitutional requirements, what level of need is required for the surveillance of the endeavour or activity. This does not mean that the endeavours warranting surveillance and the extent to which they warrant surveillance must be explicitly named in the law itself. However, it does mean that the legislator must provide an abstract description of the level of need for surveillance appropriate to the severity of interference in each case, while also defining sufficiently specific criteria for this purpose. 202

[…] 203-204

There is nothing to suggest that the tasks performed by the domestic intelligence services have any special characteristics that would inherently rule out the creation of such provisions ([...]). The need for secrecy does not, at any rate, generally prevent the legislator from defining abstract standards that direct and limit the actions of the administration. [...] 205

(2) The surveillance measure must furthermore be necessary to investigate the endeavour in the individual case (cf. BVerfGE 130, 151 <206>; 155, 119 <189 para. 151>; 156, 11 <56 para. 119>). In order for the surveillance measure to be proportionate, the sought intelligence must have specific relevance for the further investigation of anti-constitutional endeavours. It would thus be impermissible for a domestic intelligence service to carry out a measure on a purely speculative basis without being able to state how the measure is supposed to contribute to the investigation and without being able to substantiate this on the basis of factual indications. If a measure is directed against certain individuals, the surveillance of these precise individuals must contribute to the investigation. The urgency of a measure can decrease, the longer it continues without (yet) having produced any meaningful intelligence for the further investigation of anti-constitutional endeavours. The quality of the obtained intelligence must be evaluated on an ongoing basis (cf. Art. 19(2) fifth sentence BayVSG). 206

Also, because the principle of proportionality requires that less intrusive means be chosen if such means are equally suitable for achieving the intended purpose, more intrusive surveillance measures may only be chosen if the less intrusive means available do not promise to deliver equally valuable investigative results (cf. § 8(5) BVerfSchG, § 3(2) first sentence G 10). 207

Even if a more intrusive measure does promise to deliver better surveillance results, there must be an appropriate balance between the severity of interference on the one hand and the expected gain in knowledge on the other. Even the most effective option may not be used if it does not promise to deliver results of sufficient value in relation to the severity of interference with fundamental rights (cf. BVerfGE 134, 141 <187 f. para. 136>; see also BVerwG, Judgment of 14 December 2020 - 6 C 11/18 -, juris, para. 22). 208

bb) The legislator must also ensure that protection is afforded to any third parties affected by the surveillance who are not themselves part of the endeavour at issue or otherwise acting in furtherance of the endeavour. In this respect, too, the principle of proportionality gives rise to particular requirements. 209

It is not viable for the surveillance work of the intelligence services to be limited with pinpoint accuracy from the outset so that only the persons directly responsible are affected. Indeed, it is also permissible, in principle, for intelligence service methods to be used against persons who are not known to be involved in endeavours or activities that warrant surveillance but who are merely expected to provide leads on extremist activities ([...]). Nevertheless, limits must be placed on the surveillance of un- 210

involved persons to ensure that any impairment of their fundamental rights is proportionate to the expected value of the intelligence sought in the individual case.

Thus, third parties may not be directly targeted by remote searches and surveillance of private homes, which are particularly intrusive. Measures involving searches of information technology systems or the surveillance of private homes may only directly target persons who are responsible for dangers. However, the surveillance of a third party's home may be authorised (as an indirect measure) if it can be assumed, based on specific facts, that the target person will be present while the measure is carried out, will conduct conversations relevant to the observation, and the surveillance of the target person's own home would not in itself be sufficient to investigate the case. Likewise, a remote search may be extended to the information technology systems of third parties if factual indications suggest that the target person uses such systems to store relevant information, and that a remote search limited to the target person's own information technology system would not be sufficient for achieving the aims of the observation (cf. BVerfGE 141, 220 <273 f. para. 115>). 211

The ordering of other covert surveillance measures directly targeting third parties is not impermissible per se. However, as the severity of the resulting interference intensifies, the strength of the relationship between a person affected by surveillance and the group or activity under investigation must satisfy increasingly strict constitutional requirements. Vague connections are not sufficient to justify measures that result in more serious interferences with fundamental rights ([...]). The mere fact that some form of communication exists between a third party and the target person does not suffice. Instead, further indications are required suggesting that the contact is relevant to the investigation and that the surveillance measure will, with a significant degree of probability, serve the purpose of investigating the endeavour (cf. BVerfGE 141, 220 <274 f. para. 116>). 212

cc) Even if the legislator does comply with its constitutional obligations, the thresholds for surveillance specifically relating to the protection of the constitutional order are generally less nuanced than the requirements for police surveillance. This is due to the nature of the tasks performed by the domestic intelligence services, which are largely concerned with the precautionary gathering of intelligence before specific dangers arise, and for which the domestic intelligence services may be granted the necessary powers. Irrespective of the clearly recognisable efforts of the Bavarian *Land* Office for the Protection of the Constitution to impose practical constraints on its own powers in accordance with constitutional standards, further provisions are still required to ensure that the thresholds – in particular the requirement of a (heightened) need for surveillance specifically relating to the protection of the constitutional order – have their intended limiting effect in practice. Depending on the severity of interference resulting from the measure in question, the principle of proportionality in the strict sense also makes it necessary to subject the measure to *ex ante* oversight by an independent body. This independent oversight assumes particular significance given the broad nature of the thresholds that permit intelligence services to carry out 213

surveillance measures prior to the emergence of specific dangers within the meaning of police law.

(1) For the most part, the surveillance measures in question entail intrusive interferences, and it is to be expected that they will be carried out covertly and also record highly private information. According to established case-law, it is therefore imperative that measures be in principle subject to *ex ante* oversight by an independent authority, for example in the form of a judicial warrant (cf. in this regard European Court of Human Rights – ECtHR, Klass and Others v. Germany, Judgment of 6 September 1978, no. 5029/71, § 56; ECtHR <GC>, Zakharov v. Russia, Judgment of 4 December 2015, no. 47143/06, §§ 258, 275; ECtHR, Szabó and Vissy v. Hungary, Judgment of 12 January 2016, no. 37138/14, § 77). For measures relating to the surveillance of private homes, this requirement already results from Art. 13(4) GG; in general, it directly follows from the principle of proportionality (cf. BVerfGE 120, 274 <331 ff.>; 125, 260 <337 ff.>; 141, 220 <275 para. 117>; 154, 152 <292 para. 278>; 155, 119 <229 para. 253>). *Ex ante* oversight is a significant element of effective fundamental rights protection, ensuring that the interests of affected persons are sufficiently taken into account if they cannot defend their own interests before the measures are carried out, given their covert nature (cf. BVerfGE 120, 274 <331 f.>; 155, 119 <229 para. 253>). 214

The legislator must set out the requirement of independent *ex ante* oversight in a specific and clear legal framework. These provisions must oblige the authority wishing to carry out surveillance to submit a sufficiently reasoned application for a judicial warrant. Without this element, it is virtually impossible for independent oversight to be exercised effectively in practice. The authority applying for the warrant must furthermore be obliged to provide information on all aspects that are of relevance for the review. For its part, the oversight body must be obliged to produce an independent assessment as to whether the requested covert surveillance measure complies with the statutory requirements. The personnel and material conditions required for the oversight process must also be established (cf. BVerfGE 141, 220 <275 f. para. 118> with further references). 215

(2) In particular, the requirement of independent *ex ante* oversight applies to the exercise of intelligence service surveillance powers (cf. BVerfGE 154, 152 <292 para. 278 at the end>; 155, 119 <228 f. para. 252 f.>) including those of the domestic intelligence services (cf. BVerfGE 120, 274 <331 ff.>). 216

(a) Whether a covert surveillance measure needs to be reviewed by an independent body prior to being carried out depends, firstly, on the severity of the resulting interference with fundamental rights. Insofar as intelligence services are permitted to carry out covert surveillance measures, the question of whether *ex ante* oversight by an independent body is necessary must be assessed in light of the specific powers at issue and the severity of interference to which those powers give rise. Alongside the covert nature of the measure in question, the assessment must also consider 217

whether the measure is expected to concern highly private information (cf. BVerfGE 155, 119 <229 para. 253>; BVerfGE 141, 220 <275 para. 117, 294 para. 174>; CJEU, Judgment of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 inter alia, EU:C:2016:970, paras. 99, 120, 125).

218 For measures involving the surveillance of private homes, the requirement of independent *ex ante* oversight directly follows from Art. 13(3) and (4) GG. The Federal Constitutional Court has likewise held that measures involving remote searches of information technology systems carried out by a domestic intelligence service entail interferences of such severity and can intrude so deeply into the private sphere that they must be ordered by an independent authority (cf. BVerfGE 120, 274 <332>).

219 The Federal Constitutional Court has furthermore stated that independent oversight is essential under constitutional law when the Federal Criminal Police Office (*Bundeskriminalamt*) carries out certain measures such as long-term observation (especially involving the recording of images or the use of special technical means such as tracking devices), the surveillance of non-public conversations, and the use of informants (cf. BVerfGE 141, 220 <294 para. 174>). It is true that the resulting interference with fundamental rights is less severe if such measures are carried out by the domestic intelligence services, which do not have their own operational follow-up powers, rather than by the Federal Criminal Police Office (see para. 157 ff. above). Yet since the threshold is defined in less nuanced terms for the domestic intelligence services, there is still a particular need for independent *ex ante* oversight (see para. 222 below). If independent *ex ante* oversight were nonetheless to be considered unnecessary here given that domestic intelligence services have no operational follow-up powers ([...]), it would then be necessary to ensure that independent oversight is exercised prior to any information being shared with other bodies, in order to prevent the oversight mechanisms applicable to data collection by other authorities from being circumvented.

220 However, not all the covert surveillance measures of the domestic intelligence services are so intrusive as to require independent *ex ante* oversight in order to comply with constitutional law. One factor here is the duration of the measure. If a surveillance measure extends over a longer period, the resulting interference with fundamental rights can evolve over time from being relatively mild at first to eventually becoming so severe that external oversight becomes necessary, despite having initially been considered unnecessary (cf. BVerfGE 141, 220 <294 para. 174>; see also BVerfGE 112, 304 <318 f.>). Long-term surveillance measures that are so intrusive even at the beginning that independent *ex ante* oversight is required from the outset must be subjected either to time limits or repeated oversight. This is because if oversight is to be exercised responsibly, the resulting assessment – which must always include a prognosis of the measure's effectiveness – only retains its validity for a relatively short period, given the intense nature of the interference and the high-ranking legal interests at issue (cf. BVerfGE 109, 279 <361>).

(b) The involvement of external bodies in the oversight process is not precluded by the structure and nature of intelligence service activities. It is true that factual evidence is relatively scarce in the precautionary field in which the domestic intelligence services operate, with the result that assessments tend to draw more heavily on experience, specialist knowledge and general intelligence findings than is the case with the work of public security authorities. These are resources that an external body would not directly have at its disposal. However, no plausible explanation was given during the present constitutional complaint proceedings, nor is it otherwise discernible why the domestic intelligence services, despite the particularities of their work, would not be able to demonstrate to an external body, prior to carrying out a measure, that the statutory requirements (specific to the protection of the constitutional order) have been satisfied. Even if the domestic intelligence services do assess indicators of suspicious activity mainly on the basis of knowledge they have accumulated as an intelligence service ([...]), this does not absolve them from having to explain this knowledge – and the resulting assessments of suspicious circumstances based on specific facts – in a way that would at least enable an external body to verify the plausibility of the assessments. 221

Since a situation involving danger within the meaning of police law is not required, and measures are instead contingent upon the presence of factual indications suggesting a need for surveillance specifically relating to the protection of the constitutional order (or a heightened need depending on the severity of interference in the particular case), it is necessary to ensure that action is not taken on the basis of mere supposition, speculation and conjecture without any foundation in observable fact. Thus, if indications suggesting a need for surveillance specifically relating to the protection of the constitutional order are to be relied upon, they must be in the form of concrete and sufficiently tangible circumstances that are capable of establishing a suspicion that an anti-constitutional endeavour exists (cf. BVerwG, Judgment of 14 December 2020 - 6 C 11/18 -, juris, para. 23). A domestic intelligence service must be able to account for such indications both internally and – within the scope of independent oversight – externally before carrying out a measure (cf. BVerwG, Judgment of 14 December 2020 - 6 C 11/18 -, juris, para. 24 f. with further references). If a domestic intelligence service is unable to demonstrate to an independent body that the indications required under constitutional law are present, the constitutionally required threshold for exercising the surveillance powers in question is unlikely to have been reached. The element of self-regulation associated with having to provide such justification takes on particular importance in view of the fact that intelligence services typically operate in secret, which limits the effectiveness of judicial review and restricts the ability of the courts to further specify the prerequisites for interference with fundamental rights (cf. BVerfGE 141, 220 <265 para. 94>; […]). Requiring such justification serves to prevent action being taken on the basis of mere supposition and thereby ensures that the threshold for the exercise of surveillance powers specifically relating to the protection of the constitutional order is complied with. 222

[…] 223

(c) The fact that the work carried out by the domestic intelligence services is subject to long-term confidentiality requirements does not rule out the involvement of external bodies in the oversight process. Certainly, it is conceivable that when applying to carry out a surveillance measure, a domestic intelligence service may have to disclose intelligence strategies, the revealing of which would be subject to numerous conditions. It has been argued that the involvement of the courts might cause problems in this respect ([...]). In principle, however, constitutional law does not dictate that the oversight must be carried out by a court (although see Art. 13(4) first sentence GG). It would not appear to be inherently impossible for the legislator to establish independent bodies that meet the secrecy requirements. This is evidenced, for example, by the statutory provision obliging the Article 10 Committee (*G 10-Kommission*) to maintain secrecy with regard to its activities (cf. § 15(2) G 10). Furthermore, the oversight process must not in principle be allowed to be obstructed by the third party rule. This can be ensured by designing the process in accordance with strict secrecy requirements and by reaching agreements with foreign intelligence services (cf. BVerfGE 154, 152 <296 ff. para. 292 ff.> for specific details; cf. also BVerfGE 143, 101 <151 ff. para. 163 ff.>). 224

4. Proportionality (in the strict sense) of the further use and sharing of data

The principle of proportionality in the strict sense also places special requirements on the statutory provisions governing the powers of data processing and sharing (see para. 170 ff. above for the background). The constitutional requirements applicable to the further use and sharing of data collected by the state are informed by the principles of purpose limitation and change in purpose. A distinction must be made between further use by the same authority within the scope of the original purpose (see a) below) and further use for a different purpose, either by the same or another authority (see b) below). 225

a) In principle, the authority that collected the data is not required to provide separate justification for a further use of the data if such use is based on the specific grounds that justified collecting the data in the first place. However, if the legislator permits a further use of data beyond the specific grounds that prompted the original data collection and beyond the reasons that justified the original data collection, it must create a separate statutory basis to that end. A distinction must then be made between further uses that serve the same purpose as the original data collection (cf. BVerfGE 141, 220 <324 para. 278 ff.>) and further uses for purposes other than those for which the data was originally collected (cf. BVerfGE 141, 220 <326 ff. para. 284 ff.>; see para. 229 ff. below). Both require separate justification. The sharing of data with another authority constitutes a change in purpose, because a further use of data may only be regarded as serving the original purpose if it is carried out by the same authority (cf. BVerfGE 141, 220 <325 para. 279>; […]). 226

If the legislator permits an authority to make further use of its own collected data 227

beyond the specific investigation that prompted the original data collection but within the scope of the original purpose, such use may be based on the reasons that justified the original data collection and is not subject to the constitutional requirements applicable to a change in purpose (cf. BVerfGE 141, 220 <325 para. 278>). In order for the same authority to use the collected data in a new investigation, it is sufficient that the data provides sufficient leads for further investigations while still serving the same purpose as the original data collection (cf. BVerfGE 141, 220 <325 para. 279>).

However, with regard to data originating from surveillance of private homes and remote searches, the principle of purpose limitation gives rise to more stringent requirements. In keeping with the prerequisites for the collection of data in those cases, any further use of the data in a new investigation only satisfies the purpose limitation if it is necessary to avert an acute or at least an identifiable danger respectively. The extraordinary severity of interference resulting from this type of data collection is reflected in a particularly narrow limitation of any further use of the obtained data, which is subject to the prerequisites and purposes specified for the original data collection. Information thus obtained may not be used to provide leads for further investigations unless an acute or at least an identifiable danger is present (cf. BVerfGE 141, 220 <326 para. 283>). 228

b) The legislator may also allow further uses of the data for purposes other than those for which the data was originally collected. This involves a change in purpose. It must be ensured that the severity of interference resulting from the data collection is also taken into consideration with regard to the new data uses (cf. BVerfGE 141, 220 <326 f. para. 284> with further references). The applicable standard here is the criterion of a hypothetical recollection of the data (see aa) below). Based on this criterion, the data sharing requirements may differ according to which body the data is shared with (see bb) below). 229

aa) (1) If personal data collected by an authority is shared with another body, this amounts to a separate interference with fundamental rights. Such interferences must be measured against the fundamental rights which the original data collection interfered with (BVerfGE 154, 152 <266 para. 212> with further references). In substantive terms, both the statutory authorisation for data sharing and the specific data sharing measure must satisfy the proportionality requirements. The sharing of the data must be suitable, necessary and proportionate in the strict sense for achieving a legitimate purpose. 230

In order to determine whether a data sharing measure is proportionate in the strict sense, the criterion of a hypothetical recollection of the data must be applied. Based on this criterion, it is necessary to determine whether it would be permissible, under constitutional law, to collect the relevant data again for the changed purpose using comparably intrusive methods (cf. BVerfGE 141, 220 <327 f. para. 287>; 154, 152 <266 f. para. 216> with further references; 156, 11 <49 f. para. 99>; established case-law). This depends on whether, under the given circumstances, the receiving 231

body could have been permitted to collect the data itself using comparably intrusive methods as the original interference. In light of the foregoing, requirements must be set regarding both the legal interests to be protected and the thresholds for the use of powers, in this case thresholds for data sharing (BVerfGE 154, 152 <268 para. 220>; established case-law). Any new use of the data must serve to protect legal interests or detect criminal acts of such weight that it would be justified for the receiving body to collect the data itself using comparably intrusive methods as the intelligence service's original surveillance (cf. BVerfGE 141, 220 <327 para. 288>; 154, 152 <269 para. 221>; 156, 11 <55 para. 116>). Likewise, any sharing of the data must in principle be based on grounds that would provide justification, under constitutional law, for the receiving body to collect the data itself using equally intrusive methods as the original data collection (cf. BVerfGE 133, 277 <329 para. 123>; 154, 152 <269 f. para. 222>; 156, 11 <55 para. 117 f.>). The principle of a hypothetical recollection of data is not applied rigidly in a schematic manner and does not preclude the possibility that further aspects may be taken into consideration (cf. BVerfGE 156, 11 <50 para. 100> with further references).

(2) The criterion of a hypothetical recollection of the data is, in principle, also applicable to data sharing by the intelligence services, including by the domestic intelligence services (cf. BVerfGE 154, 152 <266 f. para. 216, 327 f. para. 287>; 156, 11 <1st headnote>; […]). Contrary to the Bavarian *Land* Government's assessment, the particular constitutional requirements that apply to statutory provisions governing the sharing of information obtained by an intelligence service are not rendered ineffective by the fact that the domestic intelligence services are increasingly involved in the early detection of dangers (cf. BVerfGE 156, 11 <50 f. para. 104 f.>) and that they collect data precisely for the purpose of then being able to share the data with other bodies. Here too, the sharing of data with another authority involves a change in purpose that requires justification under constitutional law. This is because the sharing of personal data with another authority always constitutes a separate interference with fundamental rights (cf. BVerfGE 154, 152 <266 para. 212> with further references; established case-law). It also constitutes a change in purpose, because a further use of data may only be regarded as serving the original purpose if it is carried out by the same authority (cf. BVerfGE 141, 220 <325 para. 279>). 232

It is true that, when deciding on the Federal Intelligence Service's strategic surveillance of foreign telecommunications, the Federal Constitutional Court found that the purpose of data collection had, in that particular case, largely merged with the purpose of sharing the data with other bodies: the Federal Intelligence Service was found to have far-reaching intelligence-gathering powers enabling it to identify important information from a large volume of largely unstructured data before any operational action is taken. As the Court observed, a key purpose of such data collection lies in distinguishing between relevant and irrelevant data in order to determine what information is provided to the government and, as the case may be, to further bodies that have executive powers. Yet the Court did not find that the sharing of such data 233

should be exempt from any special requirements. On the contrary, the Court concluded that the provisions on data sharing must ensure that intelligence obtained by the Federal Intelligence Service may only be used further if, under the general requirements arising from the rule of law, it would be permissible to collect the data for the purpose for which it is being shared (cf. BVerfGE 154, 152 <267 f. para. 218>; cf. also BVerfGE 100, 313 <367>).

bb) Based on the criterion of a hypothetical recollection of the data, the data sharing requirements may differ according to which body the data is shared with. Whether data sharing is justified depends on whether the receiving authority could have been permitted to collect the same data itself for the purpose for which the data is being shared, using comparably intrusive methods as the domestic intelligence service's original surveillance. This also depends on the powers that could be granted to the receiving authority under constitutional law. If the receiving authority has operational follow-up powers, the possibility that it could directly carry out follow-up measures itself means that stricter requirements must generally be applied to a hypothetical recollection of the data – and accordingly to a sharing of the data – than if the receiving authority has no further operational powers. In the present case, the only issue that needs to be decided is the sharing of information obtained using intelligence service methods. 234

(1) The sharing of personal data originally collected by an intelligence service, or information derived therefrom, with a public security authority is subject to particularly stringent requirements if the public security authority has coercive operational powers. Ultimately this requires that a particularly weighty legal interest (see (a) below) be at risk from at least an identifiable danger (see (b) below). 235

(a) (aa) The sharing of personal data originally collected by an intelligence service, or information derived therefrom, with a public security authority must serve a particularly weighty legal interest. An exceptionally significant public interest in data sharing is therefore required (cf. BVerfGE 133, 277 <329 para. 123>; 154, 152 <268 para. 219>; 156, 11 <51 f. para. 105, 55 para. 116>). 236

For the sharing of data obtained using the particularly intrusive surveillance powers predominantly at issue here, this requirement already stems from the fact that such surveillance powers are generally only granted for the purpose of protecting legal interests of particular importance. If a public security authority with operational powers were to collect the data itself using particularly intrusive surveillance powers, this collection of data would have to serve a particularly weighty legal interest (cf. BVerfGE 141, 220 <270 f. para. 108>). The same applies to the sharing of data with a public security authority. 237

Even if the data originates from an intelligence service surveillance measure that in itself entailed only minor interference with fundamental rights, the data may only be shared with a public security authority for the purpose of protecting legal interests of particular importance. According to the criterion of a hypothetical recollection of the 238

data, information may not be differentiated based on the severity of the individual measure used to obtain it. This is due to the special nature of the tasks performed by the intelligence services (cf. BVerfGE 133, 277 <329 para. 123>; 154, 152 <268 para. 219>; 156, 11 <51 f. para. 105>). If an individual data collection measure that entails only minor interference were to be viewed in isolation, the overall interference resulting from the broad-ranging and, in some cases, low-threshold surveillance activities of the intelligence services would not be fully accounted for.

239 Intelligence services derive their knowledge from a wealth of data, which they gather on a precautionary basis long before specific dangers arise or operational action is taken, and which they combine with other data and with intelligence from other bodies, filtering the data so that any relevant information can be extracted and also shared. This is a particular characteristic of their activities (cf. BVerfGE 154, 152 <267 f. para. 218>). […]

240 They have broad data collection powers which in some cases are neither limited to specifically defined areas of activity, nor subject to detailed rules regarding the methods that may be used or the persons that may be targeted (cf. BVerfGE 133, 277 <325 para. 117>). For example, if a domestic intelligence service wishes to carry out a covert surveillance measure that only entails minor interference with fundamental rights, all that is required is an “ordinary” need for surveillance specifically relating to the protection of the constitutional order. No indications of danger in the police sense are required, nor must there be a “heightened” need for surveillance specifically relating to the protection of the constitutional order. For the surveillance measure to be permissible, it is sufficient that the suspicion of a relevant endeavour’s existence is established by indications in the form of concrete and sufficiently tangible circumstances, even if the endeavour in question does not currently exhibit any particular potentiality (see para. 185 f. above). Also, if an intelligence service’s surveillance measure entails only minor interference with fundamental rights, indications that the targeted persons bear specific responsibility for the endeavour are not necessarily required (see para. 210 ff. above). Yet in other areas of public security law, ignoring the element of responsibility would be fundamentally incompatible with the constitutional requirements for state surveillance – at least in cases where the grounds for interference have not been specified to any meaningful degree (cf. BVerfGE 150, 244 <297 para. 142> - Automatic number plate recognition in Bavaria). The fact that intelligence services are permitted to engage in precautionary surveillance long before any specific dangers arise also justifies the broad substantive scope of their activities. Rather than being defined by specific dangers to particular legal interests, their activities are roughly circumscribed in the potentially vague terms of general threats to comparatively abstract legal interests. Furthermore, the broad-ranging surveillance activities of the intelligence services are largely conducted in secret. Intelligence services generally collect data covertly. They are not subject to the principle of the overtness of data collection and are largely exempt from transparency and notification requirements vis-à-vis affected persons. Accordingly, individuals have few possibilities

to obtain legal protection (BVerfGE 133, 277 <325 f. para. 117>).

Even if an individual data collection measure entails only minor interference with fundamental rights in itself, it must nonetheless be justified in accordance with strict constitutional requirements because the underlying powers that authorised the measure in the first place allow the domestic intelligence services to engage in the largely covert and broad-ranging collection, evaluation and processing of data without requiring any specific threat to a legal interest and, in some cases, without even requiring that the targeted persons bear any element of responsibility. Ultimately, a certain tension exists between such intelligence-gathering activities and the fundamental rights standards that usually apply to state action in a democratic state under the rule of law. The fact that domestic intelligence services, operating largely in secret and prior to the emergence of any specific danger, can obtain large quantities of personal data under relaxed conditions, and can use this data to derive information about individual citizens, is only justifiable in view of the special tasks they perform and the particularly important legal interests they serve to protect (cf. BVerfGE 133, 277 <329 para. 123>). Police authorities could not, under any circumstances, be granted such powers due to the nature of their remit. 241

This does not prevent domestic intelligence services from sharing data with public security authorities from the outset, because the criterion of a hypothetical recollection of the data is not applied rigidly in a schematic manner. Data sharing is not inherently ruled out here simply because the receiving authority, on account of its different remit, is not empowered to collect the same data as the authority sharing the data (cf. BVerfGE 141, 220 <328 para. 287>; 154, 152 <268 para. 219>; 156, 11 <50 para. 100>). However, the criterion of a hypothetical recollection of the data gives rise to stringent requirements regarding the purpose for which the shared data is to be used. Any change in purpose requires that the new use of the data serves to protect legal interests of such weight that it would be justified, under constitutional law, to collect the data again using comparably intrusive methods as the original data collection (cf. BVerfGE 141, 220 <328 para. 288>). Accordingly, data may only be shared with a public security authority for the purpose of protecting an exceptionally significant public interest. Under constitutional law, legal interests of lesser importance do not provide sufficient justification to exercise such far-reaching powers of covert data collection and intelligence gathering – not even if the information originates from an individual data collection measure that entailed only minor interference with fundamental rights. Neither an intelligence service nor any other type of authority may be permitted to carry out such measures in order to protect legal interests of lesser importance. The same applies to data sharing. Here, the criterion of a hypothetical recollection of the data requires that data only be shared to protect legal interests of particular importance, even if the data originates from a measure that entailed only minor interference with fundamental rights. 242

(bb) Particularly weighty legal interests in this sense include life, limb and liberty of the person, as well as the existence or security of the Federation or a *Land* (cf. BVer- 243

fGE 156, 11 <55 para. 116>). Data sharing may also be justified by the protection of assets of substantial value, the preservation of which is of public interest (cf. BVerfGE 141, 220 <296 para. 183>). This must be narrowly interpreted as meaning significant infrastructure facilities or other sites that are vital for society (cf. BVerfGE 133, 277 <365 para. 203>). Data sharing does not, however, have to serve the same legal interest as the intelligence service's original surveillance measure (cf. BVerfGE 154, 152 <269 para. 221>).

Nor does the legislator, when formulating the provisions on the sharing of intelligence service data for public security purposes, necessarily have to explicitly state the required legal interest. It may instead link the data sharing requirements to certain criminal offences (cf. BVerfGE 154, 152 <269 para. 221>). If, rather than explicitly naming the legal interests to be protected, the legislator instead refers to the type of criminal offences to be prevented, the weightings that apply to data collection under criminal procedural law must be applied accordingly. Where the legislator uses criminal offences as prerequisites for data sharing, preventive and repressive tasks are treated in the same way (cf. BVerfGE 141, 220 <348 para. 347>). However, the categories of considerable, serious and particularly serious criminal offences that apply to the sharing of data originally collected by a police authority are not applicable when data collected by an intelligence service is shared with a public security authority. Rather, the requirement is always that data sharing serve an exceptionally significant public interest (see para. 238 ff. above). This is equivalent to limiting the sharing of data to cases involving particularly serious criminal offences (cf. BVerfGE 154, 152 <269 para. 221 at the end>). 244

(b) The sharing of data by a domestic intelligence service with a public security authority must be limited by a data sharing threshold that requires the presence of at least an identifiable danger (cf. BVerfGE 141, 220 <272 f. para. 112>). 245

It is true that domestic intelligence services often share information they have obtained from their broader covert surveillance activities rather than from any one individual data collection measure, and that police authorities could not, under any circumstances, be granted such powers due to the nature of their remit (see para. 158 above). Yet here too, data sharing is not inherently ruled out simply because the receiving authority, on account of its different remit, is not empowered to collect the same data as the authority sharing the data (cf. BVerfGE 141, 220 <328 para. 287>; 154, 152 <268 para. 219>). From the outset, public security authorities may not be granted powers as broad as those granted to the domestic intelligence services. The threshold for sharing data with a public security authority must therefore satisfy constitutional requirements which, in the public security domain, would otherwise apply to covert surveillance measures of a highly intrusive nature (cf. BVerfGE 154, 152 <268 para. 219>). The presence of at least an identifiable danger is therefore required (on this point, see BVerfGE 141, 220 <271 ff. para. 109 ff.>). 246

The lowered threshold that applies when the Federal Criminal Police Office shares 247

its own originally collected data with other bodies (cf. BVerfGE 141, 220 <328 f. para. 289 f.>) is not applicable when a domestic intelligence service shares data with a public security authority. When the Federal Criminal Police Office shares data, it is normally sufficient under constitutional law that the data creates a specific basis for further investigations – either by itself or in combination with other information available to the authority. In this particular context, the legislator may in principle allow a change in purpose if the data concerns information that results, in the individual case, in a specific basis for further investigations aiming to avert impending dangers that may emerge at least in the medium term (cf. BVerfGE 141, 220 <329 para. 290>).

248 The lowered threshold that applies to data sharing by the Federal Criminal Police Office is not, however, applicable here. Where data originally collected using intelligence service methods is shared with a police authority, the legislator is obliged to set the same thresholds that would apply if the police authority were to originally collect the data itself – even for measures resulting in interferences of lower severity than surveillance of private homes and remote searches (cf. BVerfGE 141, 220 <329 para. 291>). The relaxed conditions for changes in purpose outlined in the Court's judgment on the Federal Criminal Police Office Act must be viewed against the backdrop of the data originally being collected by the Federal Criminal Police Office, which is bound by the thresholds generally applicable to public security authorities when carrying out such data collection measures. However, if the further use concerns data that was originally collected not by a public security authority but by an intelligence service, the original data collection is not subject to any such limitation because constitutional law does not require that intelligence services observe the same thresholds as public security authorities, nor does ordinary law contain anything to this effect (see para. 159 above). Yet since intelligence services carry out data collection measures in accordance with modified requirements, it is necessary to ensure that data sharing with a public security authority does not lead to a situation in which the requirements applicable to public security authorities can be circumvented (cf. BVerfGE 154, 152 <267 f. para. 218 f.>; 156, 11 <51 f. para. 105>). For the sharing of data collected by an intelligence service with a public security authority, the applicable standard must therefore be the general threshold for the exercise of covert surveillance powers by a public security authority (cf. BVerfGE 154, 152 <269 para. 222>; 156, 11 <55 para. 118>). This requires the presence of a specific or identifiable danger respectively (cf. BVerfGE 141, 220 <272 f. para. 112>) or, in the context of the surveillance of private homes, an acute danger (cf. Art. 13(4) GG). 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, is not affected (BVerfGE 154, 152 <272 f. para. 230>).

249 (2) The constitutional requirements that apply to statutory provisions on data sharing for prosecution purposes are likewise based on the criterion of a hypothetical recollection of the data.

(a) In general, data originally collected by an intelligence service may only be shared for the purpose of protecting an exceptionally significant public interest (see para. 236 ff. above). 250

With measures that serve prosecution purposes and are therefore repressive, the seriousness of the relevant criminal offence is a key factor. The legislator has divided such criminal offences into different categories – considerable, serious and particularly serious criminal offences – and has defined each category in greater detail (cf. BVerfGE 141, 220 <270 para. 107>). Data collected by a domestic intelligence service may only be shared for the purpose of protecting an exceptionally significant public interest, and thus only for the purpose of prosecuting a particularly serious criminal offence (cf. BVerfGE 154, 152 <269 para. 221>). 251

(b) Where data originally collected by an intelligence service is shared for prosecution purposes, the legislator is obliged to set a threshold requiring the presence of specific facts capable of establishing a suspicion. This means that concrete and relatively tangible circumstances capable of supporting such a suspicion are required (cf. BVerfGE 154, 152 <269 f. para. 222>; 156, 11 <51 f. para. 105, 56 para. 120>; BVerfGE 100, 313 <392>). […] 252

Here again, the threshold for data sharing is not subject to the lower standards outlined in the Court's judgment on the Federal Criminal Police Office Act (cf. BVerfGE 141, 220 <328 f. para. 289 f.>) that deviate from the criterion of a hypothetical recollection of the data. [...] 253

(3) The sharing of data collected by an intelligence service with any other body is likewise subject to the criterion of a hypothetical recollection of the data (cf. BVerfGE 156, 11 <55 para. 117>) as a manifestation of the more general principle of purpose limitation under data protection law ([...]). Here too, data sharing must always serve a particularly weighty legal interest (see (a) below). Nonetheless, the threshold for data sharing may be lower here than when data is shared for public security or prosecution purposes if the receiving authority, like the domestic intelligence service itself, has no operational follow-up powers of its own (see (b) below). 254

(a) Data sharing with any other body is likewise subject to the requirement that information and personal data collected by a domestic intelligence service only be shared for the purpose of protecting a particularly weighty legal interest. 255

The far-reaching powers that allow domestic intelligence services to secretly gather large amounts of information, combining and filtering the data in order to extract valuable intelligence, may not be exercised to protect legal interests of lesser importance – not even if the information originated from an individual data collection measure that entailed only minor interference with fundamental rights. This also applies to other bodies that have no operational powers. For legal interests of lesser importance, data sharing is not therefore permissible (see para. 238 ff. above for further details). 256

(b) The provision setting out the data sharing threshold must state the grounds that 257

provide justification for data sharing. These grounds must be such that the receiving authority could have been authorised to collect the data itself using comparably intrusive methods as the original data collection measure. Here too, the severity of interference resulting from a hypothetical recollection of the data depends on whether the receiving authority has operational follow-up powers at its disposal when using the data. According to general principles, the interference with fundamental rights is less intrusive if the authority does not have operational follow-up powers (see para. 159 above for details).

If the receiving body has operational powers, the same principle applies as when data is shared with a police authority: there is no scope for relaxing the threshold below the requirement of a specific or identifiable danger. If, on the other hand, the receiving body has no operational follow-up powers, a lowering of the threshold may be permissible depending on the severity of the original data collection measure. Just as the intelligence services may be granted further data collection powers because they do not have any operational follow-up powers, so too may the legislator grant further data collection powers to other bodies if they also have no operational follow-up powers. Nonetheless, it remains imperative that the purpose of data sharing is limited to that of serving an exceptionally significant public interest (see para. 236 ff. above). Depending on the specific circumstances, data sharing may then be possible if the receiving body intends to use the information in order to carry out its own tasks relating to the protection of the constitutional order and if there are sufficient factual indications in that particular case to suggest that the information is required in order to investigate a specific activity or group that warrants surveillance by an intelligence service. 258

However, this does not justify a general relaxation of the requirements that apply to the sharing of data collected by an intelligence service with other bodies that have no operational follow-up powers. Account must rather be taken of the severity of interference with fundamental rights in each particular case. This is because, depending on the receiving body's remit, data sharing can still have a massive impact on the fundamental rights of the affected persons. The statutory provision authorising the sharing of data must ensure that, in such cases, data may only be shared under strict conditions. 259

(4) Where data collected by an intelligence service is shared with a foreign authority, the data sharing requirements are based on the criterion of a hypothetical recollection of the data. The sharing of data with a foreign authority also presupposes that the data be handled in accordance with basic human rights and data protection standards in the receiving state, which must be ascertained by the German state. 260

(a) Where data is shared with a foreign authority, the requirements arising from the criterion of a hypothetical recollection of the data apply (cf. BVerfGE 141, 220 <342 ff. para. 329 ff.>; 154, 152 <273 ff. para. 231 ff.>). Data sharing is allowed if it would be permissible to collect the shared data for the purpose for which it is being shared us- 261

ing comparably intrusive methods (cf. BVerfGE 141, 220 <342 f. para. 330>; 154, 152 <266 f. para. 216>). Thus, the same requirements that apply to the sharing of data originally collected by an intelligence service with bodies in Germany also apply to the sharing of intelligence data with other states (cf. BVerfGE 154, 152 <273 para. 232>). Accordingly, a domestic intelligence service is only permitted to share information with other states for the purpose of protecting an exceptionally significant public interest (see para. 236 ff. above). Furthermore, the thresholds applicable to data sharing within Germany must also be observed. For operational public security purposes, domestic intelligence services may only share data with other states if there is at least an identifiable danger (see para. 245 ff.), for prosecution purposes only if there is sufficient suspicion (see para. 252), and for intelligence service purposes only if there are sufficient factual indications that this is necessary in the individual case to investigate a specific activity or group that warrants surveillance by an intelligence service (see para. 181 ff.).

Where data is shared with other states, it is not generally permissible to lower the degree of specificity required to establish the existence of danger or the suspicion of criminal conduct, as can be done when data originally collected by a public security authority is shared (cf. BVerfGE 141, 220 <343 para. 330>; BVerfGE 141, 220 <329 para. 290 f.>) (for the corresponding situation on data sharing within Germany, see paras. 248 and 253 above). 262

The related assessment of the receiving state's prospective use of the data must respect the autonomy of the foreign legal order. When determining whether the purpose of data sharing is of comparable weight, it must be taken into account that the German legal order is dealing with another legal order whose parameters, categories and value decisions are not, and do not necessarily have to be, identical to those reflected in the German legal order and the Basic Law. The fact that purpose limitations recognised in the German legal order are not reflected, to the same extent and in an identical manner, in the foreign legal order does not preclude data sharing with that state from the outset (BVerfGE 141, 220 <343 para. 331>). 263

(b) The sharing of personal data with other states also presupposes that the data be handled in accordance with data protection standards (see (aa) below) and basic human rights standards (see (bb) below) in the receiving state, which must be ascertained by the German state (see (cc) below) (cf. BVerfGE 141, 220 <344 para. 332>). 264

(aa) In terms of data protection standards, it is not necessary that the receiving state have rules on the processing of personal data that match those within the German legal order, or that the receiving state guarantee a level of protection that is equivalent to the protection afforded by the Basic Law. In fact, the Basic Law recognises and generally respects the autonomy and diversity of legal orders, including in the context of data sharing (BVerfGE 141, 220 <344 para. 334>). The Federal Constitutional Court has highlighted that effective cooperation with the security authorities of other states can be especially significant for public security (cf. BVerfGE 154, 152 265

<279 para. 246 f.>; see also BVerfGE 141, 220 <268 para. 102>).

Nevertheless, 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 that exactly reflect those in Germany. 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 requirements as well as fundamental requirements for oversight and data security – communicated in the course of data sharing – are at least generally observed in data usage (BVerfGE 141, 220 <344 f. para. 335>). 266

In situations where no identifiable danger in the police sense is discernible, data sharing for intelligence service purposes is not precluded from the outset merely because the receiving state makes less of an organisational distinction, or no distinction at all, between intelligence services on the one hand, and police and prosecution authorities with operational powers on the other. However, data may then be shared for operational public security purposes only if there is at least an identifiable danger, for prosecution purposes only if there is sufficient suspicion, and for intelligence service purposes only if there are sufficient factual indications that, in the individual case, this is necessary in the receiving state to investigate a specific activity or group that warrants surveillance by an intelligence service. 267

(bb) It is particularly important that the shared data be handled in accordance with basic human rights standards in the receiving state. If there is reason to fear that the use of the data in the receiving state could lead to human rights violations, it must be guaranteed in particular that the data will neither be used for political persecution nor inhuman or degrading punishment or treatment (cf. Art. 16a(3) GG). Overall, 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>; cf. also BVerfGE 154, 152 <273 ff. para. 233 ff.>). 268

(cc) The sharing of personal data with other states also requires that the German state ascertain whether the data is handled in accordance with basic human rights and data protection standards in the receiving state (cf. BVerfGE 141, 220 <344 para. 332, 345 f. para. 337 ff.>; 154, 152 <275 f. para. 239>). 269

(5) When it comes to further data use by the domestic intelligence service itself, the legislator may in principle allow such use for a changed purpose if the data concerns information that results, in the individual case, in a specific basis for further investigations of endeavours that warrant surveillance. The risk of circumvention that necessitates stricter requirements for the sharing of data with other bodies (see para. 170 ff. above) does not arise here. 270

However, this does not apply with regard to information obtained from the surveillance of private homes or remote searches. In view of the particular severity of interference attached to these measures, each new use of such data is subject to the same justification requirements as the data collection itself in that the new use also requires an acute or at least an identifiable danger respectively (cf. BVerfGE 141, 220 <329 para. 291>). 271

5. Legal clarity and specificity

Statutory provisions that authorise covert surveillance must be sufficiently clear and specific (cf. BVerfGE 113, 348 <375 ff.>; 120, 378 <407 f.>; 141, 220 <265 para. 94>; 150, 244 <278 f. para. 82>; 154, 152 <237 f. para. 137>; 156, 11 <44 ff. para. 85 ff.>). The requirement of specificity mainly serves to ensure that the law subjects the government and administration to standards that direct and limit their actions, and that the lawfulness of those actions can be effectively reviewed by the courts. The legislator must draft laws as specifically as possible, taking account of the particular nature of the underlying subject matter and the purposes pursued. With regard to legal clarity, the primary focus is on the substantive comprehensibility of legislation, in particular so as to allow citizens to adapt to the possibility of onerous measures being taken against them (cf. BVerfGE 156, 11 <45 f. para. 86 f.>). The principle of legal clarity sets limits to the use of chains of statutory 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 they must not result in excessive difficulties in their practical application. Confusing, multi-level chains of statutory references are therefore incompatible with fundamental rights requirements (BVerfGE 154, 152 <266 para. 215>). 272

In general, statutory provisions authorising the covert collection and processing of data are subject to particularly stringent requirements in terms of their specificity and clarity (cf. BVerfGE 113, 348 <375 ff.>; 120, 378 <407 f.>; 141, 220 <265 para. 94>; 150, 244 <278 f. para. 82>). This reflects the fact that protection can only be effectively guaranteed against state data collection and processing activities if the underlying legislative framework is sufficiently specific. Affected persons are not usually aware that they are being targeted by covert surveillance measures and are thus seldom able to defend themselves against such measures. As a result, the contents of the relevant legislation can only be specified to a limited degree through the interplay of practical application and judicial review, and the legislator must compensate for this by ensuring that the provisions in question are sufficiently specific. The requirements vary depending on the severity of interference in each case and are thus closely linked to the respective substantive requirements of proportionality (cf. BVerfGE 141, 220 <265 para. 94>). 273

Intelligence services, including domestic intelligence services, are not exempt from the specificity requirements. Their powers, too, must be determined by law in a clear 274

and specific manner (cf. BVerfGE 154, 152 <238 f. para. 138 ff.>; see para. 199 ff. above for more details).

6. Protection of the core of private life

a) In the case of intrusive surveillance measures, the affected fundamental rights in conjunction with Art. 1(1) GG give rise to additional requirements regarding the protection of the core of private life. These requirements apply just as much to domestic intelligence services as to police authorities because the protection afforded to the core of private life includes a right to respect for one's person (*Achtungsanspruch*), which is absolute and unconditional even when set against the high-ranking tasks performed by the domestic intelligence services (cf. BVerfGE 120, 274 <335 ff.>; also BVerfGE 141, 220 <278 para. 124>). 275

The free development of one's personality within the core of private life encompasses the possibility of expressing internal processes such as emotions and feelings, as well as 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 highly personal character merely because they concern a mixture of highly personal and everyday matters. However, communication that directly concerns criminal conduct does not form part of this protected domain, not even when it also touches on highly personal matters (cf. BVerfGE 141, 220 <276 f. para. 121 f.>). 276

The protection afforded to the core of private life is strict and must not be made conditional upon a balancing against security interests under the principle of proportionality. This does not mean that every instance in which highly personal information is collected amounts to a breach of constitutional law or even a violation of human dignity. However, it does require that the protection of the core of private life be taken into account on two different levels when carrying out surveillance measures. Firstly, at the data collection stage, safeguards must be put in place to prevent the unintended collection of information relating to the core wherever possible. Secondly, at the stage of subsequent data analysis and use, the consequences of an intrusion upon the core of private life that could not be prevented despite the presence of such safeguards must be strictly minimised (cf. BVerfGE 141, 220 <278 ff. para. 126 ff.> with further references). 277

Every type of surveillance measure must respect the core of private life. If the measure in question typically leads to the collection of data relating to the core, the legislator must enact clear provisions that ensure effective protection. Where the powers in question do not entail such a risk of core violations, it is not necessary to enact such provisions. But even when exercising those powers, limits that directly arise from the Constitution regarding access to highly personal information must be respected in the individual case (BVerfGE 141, 220 <277 f. para. 123>). 278

b) The constitutional requirements for protecting the core of private life are particularly strict in the case of surveillance of private homes – a measure that reaches deep into the private sphere and intrudes upon the affected individual's personal refuge, which is of fundamental importance for safeguarding human dignity (cf. BVerfGE 141, 220 <299 f. para. 197>). 279

aa) Particular requirements apply at the data collection stage. When assessing whether there is a probability that highly private situations will be recorded, certain presumptions apply in the interest of effectively protecting the core of private life. Thus, conversations taking place in private spaces with persons enjoying the highest level of personal trust are presumed to belong to the core of private life and may not be the target of surveillance. The automatic long-term surveillance of spaces in which such conversations are to be expected is therefore impermissible. This presumption can be rebutted when specific indications suggest that certain conversations are, within the meaning of the standards set out above, directly linked to criminal conduct. Where such links exist, they are not cancelled out when the conversations in question are mixed with highly personal content. The presumption can also be rebutted by indications suggesting that the overall nature of the conversation is not actually highly confidential. However, the mere expectation that a conversation will concern both highly confidential and everyday matters is not sufficient by itself (BVerfGE 141, 220 <300 para. 198>). 280

Thus, if a surveillance measure is likely to intrude upon the core of private life, the measure may not be carried out. If, on the other hand, there are indications suggesting that certain conversations will not actually be highly confidential in nature, the measures may be carried out. However, where the measures, despite no prior indications, result in the recording of highly confidential situations, they must be discontinued immediately. If it is not clear whether a situation is highly confidential – for example due to language barriers – or if there are specific indications suggesting that, mixed in with highly private thoughts, criminal acts will also be discussed, surveillance in the form of automatic recordings may be continued (cf. BVerfGE 141, 220 <300 f. para. 199>). 281

bb) Specific constitutional requirements also arise at the stage of data analysis and use. It must be ensured that the information obtained from the surveillance measure is independently screened. This also applies to the activities of the domestic intelligence services because the protection afforded to the core of private life includes a right to respect for one's person, which is absolute and unconditional even when set against the special tasks performed by the domestic intelligence services (cf. BVerfGE 120, 274 <335 ff.>). The independent screening process serves both as a review of lawfulness as well as a filter mechanism to remove highly confidential data so that, as far as possible, such data is not disclosed to the authority that carried out the surveillance. The body carrying out the independent screening must be provided with all the data originating from the surveillance of a private home (cf. BVerfGE 141, 220 <301 para. 200, 302 para. 204>; cf. foundationally also BVerfGE 109, 279 <333 f.>). 282

While the necessary oversight powers generally have to be comprehensive in scope, the Basic Law does leave room for the legislator to enact special provisions that cover exceptional cases of danger requiring imminent action (*Gefahr im Verzug*) (BVerfGE 141, 220 <302 para. 204>).

Although the case-law of the Federal Constitutional Court emphasises the necessity of having the screening process carried out by an independent body, this does not inherently exclude the possibility of using an automated screening process, provided that such a process is technically feasible and reliable (or eventually becomes so at some point in the future). The decisive point is that no data relating to the core of private life may be disclosed to the authority that carried out the surveillance, beyond any information unavoidably revealed at the data collection stage (cf. BVerfGE 141, 220 <308 para. 224>). The screening process, which is designed to protect the core of private life during the data analysis stage, must not provide the authority that carried out the surveillance with an opportunity to derive (further) knowledge from the data. 283

c) In the case of covert access to information technology systems (i.e. remote searches) as well, there is typically a risk of highly confidential data being recorded, with such measures bearing a particularly close connection to the core of private life. Express statutory safeguards to protect the core are therefore necessary here too. However, the requirements are not the same in every respect as those for the surveillance of private homes. The protection in respect of remote searches is concentrated less at the data collection stage and more at the subsequent stage of data analysis and use. This is due to the technical nature of remote searches. In the context of such measures, protecting the core of private life involves preventing the retrieval of highly confidential information from within an existing comprehensive data pool of digital information that, taken as a whole, is not typically of the same private nature as a person's behaviour or communication within the home. As a result, the constitutional requirements for protecting the core of private life at the data collection stage are somewhat lower. 284

Yet for remote searches too, it must still be ensured that the collection of information attributed to the core is avoided as far as is possible from a technical and investigative perspective. Available technical means must be used to implement such protection. Where these technical means make it possible to identify and isolate highly confidential information, access to this information is prohibited. 285

If, however, data relating to the core cannot be filtered out before or at the time of data collection, remote searches are nevertheless permissible even if there is a probability that highly personal data, too, might incidentally be collected. In this respect, the legislator must take into account the need for protection of affected persons by putting safeguards in place at the stage of data analysis and use, and by minimising the impact of remote searches. It is critically important here to have an independent body carry out a screening process, removing any information relating to the core be- 286

fore the authority that carried out the surveillance can derive knowledge therefrom or make use thereof (cf. for the topic as a whole, BVerfGE 141, 220 <306 f. para. 218 ff.>; in the particular context of domestic intelligence services, BVerfGE 120, 274 <338 f.>).

7. Combined effect of surveillance measures

287 The combined effect of different surveillance measures gives rise to distinct constitutional limits. Surveillance which takes place over an extended period and covers almost every movement and expression of the person under surveillance, and which could be used as the basis for creating a personality profile, is incompatible with human dignity. Where modern investigation methods are used, especially methods that cannot be perceived by the persons affected, the potential harm inherent in “additive” interferences with fundamental rights must be taken into account to ensure that the overall extent of the surveillance remains limited (cf. BVerfGE 141, 220 <280 f. para. 130> with further references). Constitutional law requires that authorities directly observe this aspect of the proportionality principle of their own accord when exercising their surveillance powers. It is not therefore necessary to put any further statutory provisions in place.

288 This also applies to the surveillance powers of domestic intelligence services. If a domestic intelligence service carries out a number of different surveillance measures in parallel, it must ensure that the cumulative effect of these measures does not violate the principle of proportionality in the individual case. As to how the required coordination of different measures is handled internally within the particular domestic intelligence service itself, the legislator is entitled to assume that this issue is adequately taken care of by the service’s management within the scope of its executive responsibilities (cf. BVerfGE 141, 220 <317 para. 254>; on the implications for oversight, see para. 290 below).

8. Procedural requirements

289 The principle of proportionality in the strict sense gives rise to procedural requirements concerning the design of surveillance powers. These requirements also apply to the domestic intelligence services (foundationally, BVerfGE 65, 1 <44, 46>). Apart from necessitating a system of independent *ex ante* oversight, which is a critically important safeguard to ensure that fundamental rights are protected in the field of domestic intelligence (see para. 213 ff. above for more details; cf. BVerfGE 141, 220 <275 para. 117>), the principle of proportionality in the strict sense also requires that statutory provisions set out notification requirements and rights to information in principle (cf. BVerfGE 133, 277 <369 para. 213>; 141, 220 <282 f. para. 136 f.>; established case-law) as well as reporting obligations (cf. BVerfGE 133, 277 <372 para. 221 f.>; BVerfGE 141, 220 <285 para. 142 f.>; established case-law). However, the particular need for secrecy in this area can justify modifying these requirements (cf. on applicability and modifications in the context of the intelligence services, BVerfGE 154, 152 <287 f. para. 266 ff., 299 para. 298, 287 ff. para. 266 ff.>; cf. BVer-

fGE 133, 277 <369 para. 213>; […]).

In order to be proportionate, the covert surveillance measures at issue here also require an effective system of administrative oversight. With covert surveillance measures, the transparency of data collection and processing activities and the availability of individual legal protection can only be ensured to a very limited degree, making effective administrative oversight all the more important (cf. BVerfGE 133, 277 <369 ff. para. 214 ff.>; 141, 220 <284 f. para. 140 f.>). This in turn requires the existence of a body vested with effective powers (cf. foundationally, BVerfGE 65, 1 <46>; 141, 220 <284 f. para. 141>). To be effective, the oversight body must in principle be able to review all the surveillance measures that an authority uses against an individual. This is because the proportionality of any one particular surveillance measure partly depends on the extent to which other surveillance measures are carried out in parallel (see para. 287 f. above). If the oversight body only has a restricted amount of data at its disposal, it cannot reliably assess the extent and lawfulness of surveillance activities and the cumulative interference with fundamental rights that may occur as a result (cf. also BVerfGE 133, 277 <370 para. 216>). 290

II. Substantive constitutionality of the challenged provisions

The constitutionality of each of the powers granted to the Bavarian *Land* Office for the Protection of the Constitution depends on the fundamental rights at issue in each case and, in particular, on whether the powers in question are compatible with the principle of proportionality. The challenged powers serve a legitimate purpose and are in principle suitable and necessary for achieving that purpose (see para. 150 ff. above). However, the challenged powers are partly inconsistent with certain limits arising from the principle of proportionality in the strict sense. 291

1. Art. 9(1) BayVSG – surveillance of private homes

Art. 9(1) first sentence BayVSG is unconstitutional. Surveillance of private homes must be measured against Art. 13(1) and (4) GG. On this basis, Art. 9 BayVSG partly fails to satisfy the constitutional requirements. Although the provision does essentially require sufficient grounds for exercising the powers granted thereunder (“acute danger”), it is not aimed at the purpose of averting acute danger and it lacks the element of subsidiarity vis-à-vis public security measures taken by public security authorities. Moreover, it does not fully satisfy the constitutional requirements for protecting the core of private life applicable to the surveillance of private homes. 292

a) Art. 9(1) first sentence BayVSG authorises the Bavarian *Land* Office to carry out acoustic and visual surveillance of private homes. Surveillance of private homes by technical means interferes with the inviolability of the home (Art. 13(1) GG). The powers conferred upon the Bavarian *Land* Office to carry out such activities for preventive purposes under Art. 9(1) first sentence BayVSG must be measured against the requirements arising from Art. 13(1) and (4) GG. 293

b) Surveillance of private homes is subject to especially stringent requirements (cf. 294

BVerfGE 141, 220 <295 f. para. 180>). The surveillance of a private home involves a particularly deep invasion of the private sphere (cf. BVerfGE 141, 220 <269 para. 105>) because it permits the state to intrude into spaces that are a person's private refuge and that are closely linked to human dignity (cf. BVerfGE 141, 220 <295 para. 180> with further references). While it is clear from Art. 13(3) and (4) GG that this does not categorically rule out the possibility of surveillance, Art. 13(4) GG does give rise to more stringent criteria than the requirements generally arising from the principle of proportionality in the strict sense (see para. 181 ff. above).

aa) Art. 13(4) GG allows the acoustic or visual surveillance of a private home only for the purpose of averting an acute danger. Art. 13(4) GG formulates this particularly stringent requirement without distinguishing between the different types of authority carrying out the surveillance; it therefore also applies to domestic intelligence services (see para. 169 above). The resulting standards are not entirely satisfied by Art. 9(1) first sentence BayVSG. It is true that the threshold set by the legislator is, in principle, permissible and the legal interest to be protected is sufficiently weighty (see (1) below). Moreover, Art. 13(4) GG does not inherently exclude domestic intelligence services from being granted powers to carry out surveillance of private homes (see (2) below). In this instance, however, the powers granted to the Bavarian *Land* Office are unconstitutional because they are not explicitly aimed at the purpose of averting danger (see (3) below). Furthermore, the necessary element of subsidiarity is lacking (see (4) below). 295

(1) In principle, the legislator has designed a threshold for interference that is compatible with Art. 13(4) GG and the legal interest to be protected is sufficiently weighty. Art. 13(4) GG allows the surveillance of private homes by technical means only for the purpose of averting acute dangers to public security. 296

Acute danger within the meaning of Art. 13(4) GG is present when it can be assumed with sufficient probability that a specific situation or behaviour would cause major damage in the immediate future if the chain of events that is objectively to be expected were to unfold without intervention. The criterion of "acuteness" relates to the potential extent of the damage and the probability of such damage occurring (cf. BVerfGE 130, 1 <32>; 141, 220 <271 para. 110>). The threshold set out in Art. 9(1) first sentence BayVSG satisfies this criterion. 297

Art. 9(1) first sentence BayVSG requires that factual indications of acute danger be present. Requiring factual indications of acute danger to be present – something not included in the wording of Art. 13(4) GG – is constitutional as long as it is not understood as limiting the requirements concerning the degree of specificity that the danger must already have reached. 298

The Bavarian legislator also named sufficiently weighty legal interests in Art. 9(1) first sentence no. 1 (existence or security of the Federation or a *Land*) and Art. 9(1) first sentence no. 2 BayVSG (life, limb or liberty of the person). The same applies to Art. 9(1) first sentence no. 3 BayVSG (assets the preservation of which is of special 299

public interest), although the element of special public interest must be narrowly interpreted here as referring to assets such as significant infrastructure facilities or other sites that are vital for society (cf. BVerfGE 133, 277 <365 para. 203>; 141, 220 <287 para. 155>).

(2) The power to conduct surveillance of private homes under the conditions set out in Art. 13(4) GG may also be granted to domestic intelligence services. Art. 13(4) GG does not exclude them from the generally established possibility of carrying out surveillance of private homes ([...]). 300

(3) Art. 9(1) first sentence BayVSG is nonetheless unconstitutional insofar as it does not explicitly limit the surveillance to the purpose of averting the listed dangers. Whereas Art. 13(4) GG only allows surveillance of private homes for the purpose of "averting" acute dangers ([…]), Art. 9(1) first sentence BayVSG merely requires the presence of factual indications of acute danger to the listed legal interests, without the surveillance ultimately having to be aimed at the purpose of averting the danger. [...] The presumption that the surveillance in question is intended to serve the purpose of averting danger cannot be derived from Art. 9(1) first sentence BayVSG, given that no such wording is contained in the text itself, nor can this be deduced as an unwritten condition. This would in any case fail to satisfy the principle of specificity, which imposes strict requirements here (cf. BVerfGE 141, 220 <265 para. 94> with further references; established case-law). Rather, the legislator must explicitly formulate a provision limiting the power to carry out surveillance of private homes to the purpose of averting an acute danger (cf., e.g., § 9(2) first sentence BVerfSchG). 301

It is true that, under the currently applicable legal framework, it would not actually be possible to confer tasks involving the aversion of danger upon the Bavarian *Land* Office for the Protection of the Constitution since the performance of such tasks would require executive police powers. The fact that intelligence services are not given operational follow-up powers is an essential prerequisite for ensuring that the relevant security architecture in its current legislative form is compatible with the Basic Law (see para. 156 ff. above for more details). It would, however, be possible to enact provisions authorising the Bavarian *Land* Office to share data obtained from the surveillance of private homes with other bodies that do have direct public security powers, on condition that the surveillance was carried out for the purpose of averting an acute danger [...]. [...] 302

(4) The provision furthermore lacks the element of subsidiarity that is necessary under constitutional law (for more details, see para. 178 ff. above), as is properly included in § 9(2) first sentence BVerfSchG, for example. Domestic intelligence services may only be granted authorisation to carry out the surveillance of a private home on a subsidiary basis, i.e. only in the event that suitable police assistance for the legal interest at risk cannot otherwise be timely obtained. This is not the case here. 303

bb) The provisions in Art. 8a(1) BayVSG concerning protection of the core of private life do not entirely satisfy the applicable constitutional requirements in the case of 304

surveillance of private homes (see para. 279 ff. above).

(1) At the data collection stage, the presumption made when carrying out surveillance of a private home must favour the protection of privacy. Yet the general formulation in Art. 8a(1) first sentence BayVSG concerning the protection of the core of private life fails to explicitly mention this presumption in the constitutionally required manner. Under the legislative technique chosen here, the presumption is rather that the use of intelligence service methods is permissible unless sufficiently weighty factual indications stand in the way. [...] At any rate [...], the mere fact that this provision can be interpreted in conformity with the Constitution is not sufficient to satisfy the constitutional requirements applicable to protecting the core of private life. The provision must instead make it explicitly clear that conversations within the private home may only be the target of surveillance if the constitutional presumption in favour of the protection of privacy that is required under constitutional law – i.e. the presumption that private spaces where conversations with persons enjoying the highest level of personal trust are expected to occur belong to the core of private life and are protected as such – has been rebutted. Where powers that interfere with fundamental rights, such as the power to carry out surveillance of a private home, typically lead to the collection of data relating to the core of private life, the legislator must enact clear provisions that ensure effective protection (cf. BVerfGE 141, 220 <277 para. 122>). The law must therefore explicitly include the relevant presumption. 305

(2) At the data analysis stage, the provision does not satisfy the constitutional requirements for protecting the core of private life applicable to the surveillance of private homes either. Art. 8a(1) BayVSG does not ensure that all the information originating from the surveillance is first comprehensively screened by an independent body with regard to its relevance to the core of private life prior to the Bavarian *Land* Office obtaining access to the information. [...] 306

2. Art. 10(1) BayVSG – remote searches

Art. 10(1) BayVSG authorises the Bavarian *Land* Office for the Protection of the Constitution to use technical means to remotely access the information technology systems within a targeted person's sphere of control and to thereby retrieve and collect data without that person becoming aware of the fact (a so-called remote search). The provision must be measured against the general right of personality (Art. 2(1) in conjunction with Art. 1(1) GG) in its specific manifestation as a fundamental right to the confidentiality and integrity of information technology systems. Art. 10(1) BayVSG fails to satisfy this standard because, by making reference to the requirements set out in Art. 9(1) BayVSG, it shares that provision's deficiencies in terms of not being sufficiently aimed at the aversion of danger and in terms of lacking the element of subsidiarity. Furthermore, the protection afforded to the core of private life is inconsistent with the applicable requirements. On the other hand, the powers conferred under Art. 10(1) BayVSG are not rendered unconstitutional by any subsequent risks to information technology systems. 307

a) Remote searches interfere with the fundamental right to the confidentiality and integrity of information technology systems, which is protected under Art. 2(1) in conjunction with Art. 1(1) GG (foundationally, BVerfGE 120, 274 <302 ff.>). Art. 10 BayVSG must be measured against this fundamental right and not against the privacy of communications (Art. 10(1) GG) because rather than being limited in scope to ongoing telecommunications, it permits access to entire information technology systems (cf. Federal Constitutional Court, Order of the First Senate of 8 June 2021 - 1 BvR 2771/18 -, para. 28 with further references; established case-law). 308

b) Art. 10(1) BayVSG does not entirely satisfy the constitutional requirements. 309

aa) Domestic intelligence services are only permitted to conduct remote searches for the purpose of averting at least an identifiable danger, within the meaning of police law, to a particularly weighty legal interest. Furthermore, they may only be granted authorisation to carry out such measures on a subsidiary basis (see para. 176 ff. above for more details). 310

(1) Art. 10(1) BayVSG is constitutional insofar as it makes reference to Art. 9(1) BayVSG regarding the requirements applicable to the threshold for interference and the legal interest to be protected (see para. 296 ff. above). However, insofar as it fails to define a purpose, it does not satisfy the constitutional requirements. The reference to Art. 9(1) BayVSG means that, again, the powers conferred under Art. 10(1) BayVSG only require the presence of an acute danger to certain legal interests. This is too broad since it does not require any specific link to the purpose of averting an existing danger, which is what legitimates the interference in the first place. It is true that the Basic Law does not explicitly require that remote searches be limited to the purpose of averting danger; this contrasts with the surveillance of private homes, which is specifically linked to preventive purposes in Art. 13(4) GG. But regardless of any explicit mention in the Basic Law, constitutional requirements still make it necessary for the purpose of remote searches to be limited to the aversion of danger, because otherwise the special threshold that requires a danger within the meaning of police law would no longer serve its purpose-limiting function as is constitutionally required. If the Bavarian *Land* Office for the Protection of the Constitution were permitted to use the mere presence of a danger that has materialised (*konkret eingetretene Gefahr*) as justification for collecting and analysing information in line with its responsibilities under Art. 3 BayVSG in conjunction with § 3 BVerfSchG, the constitutionally necessary threshold for interference that requires the presence of at least an identifiable danger would be undermined because its limiting function is only effective in combination with a purpose limitation that requires measures to be aimed at averting such danger. 311

(2) Furthermore, the necessary element of subsidiarity is once again lacking (see para. 179 f. above for more details). 312

bb) The provisions in Art. 8a and Art. 10(2) first sentence no. 3 BayVSG concerning the protection of the core of private life only partially satisfy the constitutional require- 313

ments applicable to remote searches (see para. 284 ff. above).

(1) At the data collection stage, the provisions in Art. 8a(1) first sentence and Art. 10(2) first sentence no. 3 BayVSG satisfy the applicable constitutional requirements for protecting the core of private life in the case of remote searches. [...] 314

(2) At the data analysis stage, however, the provisions are insufficient for protecting the core of private life because they fail to provide for a necessary system of independent oversight in which the collected data is screened before being used. [...] 315

cc) By contrast, the fact that interferences under Art. 10(1) BayVSG entail subsequent risks to the security of the affected information technology systems does not violate constitutional law. It is true that powers to conduct remote searches do, by virtue of their very existence, present authorities with an incentive to keep open any security vulnerabilities that come to their attention so as to exploit such vulnerabilities for infiltration purposes, and that this affects the severity of the interference resulting from remote searches (cf. BVerfGE 120, 274 <326>; Federal Constitutional Court, Order of the First Senate of 8 June 2021 - 1 BvR 2771/18 -, para. 42). However, this heightened severity has already been taken into account by the stricter requirements applicable to the threshold for carrying out remote searches (cf. BVerfGE 120, 274 <325 f., 328>; 141, 220 <304 f. para. 211 f.>; Federal Constitutional Court, Order of the First Senate of 8 June 2021 - 1 BvR 2771/18 -, para. 43). […] 316

3. Art. 12(1) BayVSG – tracking of mobile devices

Art. 12(1) BayVSG authorises the Bavarian *Land* Office for the Protection of the Constitution to track mobile devices. Under this provision, the Bavarian *Land* Office is permitted to use technical means to determine the location of an activated mobile device or ascertain the number of a particular device or card, on condition that there are factual indications of a serious danger (*schwerwiegende Gefahr*) to the legal interests protected under Art. 3 BayVSG. Since this authorisation is not limited to one-off measures and therefore does not preclude the creation of movement profiles, it enables particularly intrusive interferences with fundamental rights (see a) below). In this respect, the provision fails to satisfy the justification requirements under constitutional law (see b) below). 317

a) The data collection powers conferred under Art. 12(1) BayVSG interfere with the right to informational self-determination, a right that is constitutionally protected under Art. 2(1) in conjunction with Art. 1(1) GG (see aa) below). The powers under Art. 12(1) BayVSG make it possible to create movement profiles, thereby enabling serious interferences with fundamental rights (see bb) below). 318

aa) Measures under Art. 12(1) BayVSG interfere with the rights of affected persons to informational self-determination. In an earlier decision by the Federal Constitutional Court, surveillance measures carried out on the basis of comparable powers under criminal procedural law were regarded as interfering with the general right of personality (Art. 2(1) in conjunction with Art. 1(1) GG) in its manifestation as a fundamental 319

right to informational self-determination (cf. Federal Constitutional Court, Order of the First Chamber of the Second Senate of 22 August 2006 - 2 BvR 1345/03 -, para. 64 ff. - on so-called IMSI catchers <see para. 323 below>; cf. also Federal Court of Justice – *Bundesgerichtshof* – BGH, Order of 8 February 2018 - 3 StR 400/ 17 -, Decisions of the Federal Court of Justice in Criminal Matters – *Entscheidungen des Bundesgerichtshofes in Strafsachen* – BGHSt 63, 82 <84 f. para. 5 f.> - on so-called silent SMS (*stille SMS*) <see para. 324 below>). The more specific fundamental right to the privacy of communications under Art. 10(1) GG was held to be inapplicable (cf. Federal Constitutional Court, Order of the First Chamber of the Second Senate of 22 August 2006 - 2 BvR 1345/03 -, para. 49 ff. with further references; […]). It is not necessary here for the Court to conclusively decide which of these two fundamental rights is applicable, since measures under Art. 12(1) BayVSG interfere in any case with the fundamental right to informational self-determination. Furthermore, the requirements derived from Art. 2(1) in conjunction with Art. 1(1) GG are largely consistent with the more specific guarantees arising from Art. 10 GG (cf. BVerfGE 155, 119 <170 para. 100> with further references; see also Gurlit, NJW 2010, 1035 <1037 ff.>; […]).

bb) Art. 12(1) BayVSG authorises serious interferences with fundamental rights. The severity of this interference depends on the operational possibilities that the provision opens up both in legal and practical terms. 320

(1) Given the essentially limited informative value of data collected under Art. 12(1) BayVSG, the resulting interference would not be particularly serious if the tracking activities authorised by the provision were restricted to one-off measures. However, because Art. 12(1) BayVSG is silent on the frequency of tracking activities and the overall duration of such measures, the provision allows, from the legal perspective at least, for a person's location to be repeatedly determined at short intervals. If this method is used over a longer period to track the mobile phone of a person under surveillance and to create a movement profile, the resulting interference with fundamental rights is severe (cf. BVerfGE 120, 378 <400 f., 406 f.>; 125, 260 <319 f.>; 150, 244 <285 para. 100>). 321

(2) When assessing the provision's constitutionality, the interference must be assumed to possess this high degree of severity. [...] At present, there are at least two different technical possibilities for using the powers conferred under the provision, the second of which can certainly be of practical relevance for the creation of movement profiles. 322

(a) The first possibility is to use so-called IMSI catchers. These can ascertain the international mobile subscriber identity (IMSI) stored on a mobile phone's chip card and can determine the location of an activated phone ([…]). […]. In theory, the location data collected using an IMSI catcher makes it possible to create uninterrupted movement profiles ([...]). In practice, however, this method does not appear to have any operational relevance ([...]) because it requires advance knowledge of the target 323

person's approximate location, as well as the ability to use an IMSI catcher within range of that person's mobile phone.

(b) The second way of determining the location of a mobile phone that is switched on and receiving a signal is to use the silent SMS technique. Here, a text message is sent via SMS (Short Message Service) to a mobile phone number, establishing a connection with the targeted phone without its user being aware of the fact. Upon receiving the message, the phone sends confirmation to the cell tower from which it is currently receiving a signal. This is used to generate a set of traffic data that includes the identity of the cell tower used by the phone. By retrieving this data from the network operator, it is possible to determine the mobile device's approximate location when it received the silent SMS ([...]). It is therefore a two-stage process ([...]). § 100i StPO, the provision in the Code of Criminal Procedure that corresponds to Art. 12(1) first alternative BayVSG, has been invoked as the legal basis for the silent SMS technique (cf. BGH, Order of 8 February 2018 - 3 StR 400/17 -, BGHSt 63, 82 <86 f. para. 11 ff.>; [...]). The use of the silent SMS technique and the subsequent retrieval of the generated location data make it possible to create a movement profile (cf. BGH, Order of 8 February 2018 - 3 StR 400/17 -, BGHSt 63, 82 <84 f. para. 6>). It is a comparatively straight-forward process and enables relatively accurate location tracking, especially in major conurbations where cell towers tend to be quite closely spaced ([...]). 324

(c) When formulating Art. 12(1) BayVSG, it can be assumed that the legislator only had the use of IMSI catchers in mind ([...]). [...] At present, the interference arising from Art. 12(1) BayVSG is not especially severe in the case of using IMSI catchers, given that the practical applications are limited. 325

However, the legislator's ability to envisage the extent of a conferred power's impact does not determine the severity of the resulting interference. The severity must rather be assessed in light of the possibilities for interfering with fundamental rights that the conferred power actually and presently opens up; thus the possibility of using the silent SMS technique on more than just isolated occasions also needs to be taken into consideration (see para. 324 above). The fact that the silent SMS technique and the subsequent retrieval of the location data make it possible to create a movement profile, albeit a relatively approximate one, has a serious impact on the fundamental right to informational self-determination (cf. BGH, Order of 8 February 2018 - 3 StR 400/17 -, BGHSt 63, 82 <84 f. para. 6>). Strict constitutional requirements must therefore be applied. If the legislator had wanted to limit the severity of the interference over the long term, it should have made this explicitly clear in the wording of Art. 12 BayVSG – especially in view of the fact that technical developments may lead to new capabilities. The legislator did not do this. 326

b) The provision fails to satisfy the resulting strict justification requirements under constitutional law. 327

aa) Art. 12 BayVSG does not establish sufficiently specific prerequisites for interfer- 328

ence. The principle of proportionality in the strict sense requires that authorisation to conduct a measure under Art. 12(1) BayVSG only be granted if the measure is necessary in the individual case to investigate a specific activity or group that warrants surveillance by an intelligence service. The decisive factor here is whether the intelligence sought by the measure has specific relevance for the further investigation of anti-constitutional endeavours. Since a measure of this type will usually be directed against certain individuals, the surveillance of these precise individuals must contribute to the investigation. In addition, due to the considerable potential severity of the resulting interference, authorisation to carry out such measures must be made contingent upon a heightened need for surveillance (see para. 192 ff. above for general information on the requirements).

Art. 12(1) BayVSG fails to satisfy these requirements because the prerequisites for interference are not set out in a sufficiently specific manner. The provision requires that factual indications of a serious danger to the protected elements of the constitutional order be present in order for a measure to be authorised. If danger were to be understood here in the sense used for police action, a situation would be required in which it can be assumed with sufficient probability that the chain of events that is objectively to be expected will lead, in the individual case and within the foreseeable future, to the violation of one of the designated legal interests if the situation were to unfold without intervention (cf. BVerfGE 141, 220 <271 para. 111>; see para. 158 above). As the complainants rightly submit, this threshold from the field of police action would hardly ever be reached if it were applied to the domain of the domestic intelligence services. Yet the legislator clearly did not intend to set a virtually unattainable threshold for the domestic intelligence services. The domestic intelligence services make frequent use of the powers to track mobile devices and ascertain device and card numbers (cf. Bavarian *Landtag* document, *Bayerische Landtagsdrucksache* – BayLTDrucks 17/16055, 17/22322, 18/2079 and 18/18535). It can be assumed that the legislator's intention was to make these powers effectively available to the domestic intelligence services for their surveillance work. This would clearly not be the case if the prerequisites for interference were interpreted in the sense used for police action as described above. And yet Art. 12(1) BayVSG does not contain any description of the grounds for interference that specifically relates to the protection of the constitutional order and that matches the domestic intelligence tasks performed by the Bavarian *Land* Office. The meaning of serious danger as used in Art. 12(1) BayVSG is not so obvious as to enable the substance of the provision to be understood with sufficient certainty without any further statutory specification. 329

[…] 330

[…] In view of the potential severity of interference resulting from the measures permitted thereunder, Art. 12(1) BayVSG is too unspecific. Since the provision does not exclude the long-term tracking of spatial movements and does not therefore rule out severe interferences with fundamental rights, the specificity of the prerequisites for interference must be subject to strict requirements. These requirements are not sat- 331

isfied by the element of serious danger, given that it does not contain any description of the grounds for surveillance that specifically relates to the protection of the constitutional order. It is not sufficient that, in a different case involving surveillance powers, the Federal Constitutional Court did interpret this element in a manner specifically relating to the protection of the constitutional order. Rather, if the legislator wishes to grant the Bavarian *Land* Office the powers in Art. 12(1) BayVSG, it would have to set a qualified threshold for interference specifically relating to the protection of the constitutional order. The use of such powers would require a heightened need for surveillance, and the domestic intelligence services would have to be provided with statutory direction as to when such a need arises. Such statutory direction is lacking here.

bb) To the extent that Art. 12(1) BayVSG does not explicitly preclude using the surveillance powers to carry out long-term monitoring that can lead to the creation of comprehensive movement profiles, independent *ex ante* oversight is also required due to the potentially great severity of the interference (cf. BVerfGE 141, 220 <275 para. 117, 294 para. 174>; cf. on the use of the Global Positioning System (GPS) - without reaching an unequivocal conclusion - BVerfGE 112, 304 <318 f.>). Art. 12(1) BayVSG fails to provide for such oversight. The legislator is, however, entitled to limit the scope of *ex ante* oversight to surveillance measures of a comprehensive nature. The prior independent review of one-off surveillance measures carried out under Art. 12(1) BayVSG is not essential under constitutional law due to the limited severity of the resulting interference. 332

4. Art. 15(3) BayVSG – disclosure of traffic data originating from data retention

Art. 15(3) BayVSG governs access to the data stored by service providers under data retention rules. Ultimately, the provision is incompatible with the principle of legal clarity and violates Art. 10(1) GG because it authorises the Bavarian *Land* Office for the Protection of the Constitution to access data, without service providers being obliged or even authorised under federal law to share such data with the Bavarian *Land* Office. 333

Art. 15(3) BayVSG authorises the Bavarian *Land* Office to access traffic data retained in accordance with § 113a of the Telecommunications Act (*Telekommunikationsgesetz* – TKG) in its former version (§ 175 TKG in the new version) under the conditions set out in § 113c(1) no. 2 TKG in its former version (§ 177(1) no. 2 TKG in the new version). This interferes with the privacy of telecommunications guaranteed under Art. 10(1) GG (cf. BVerfGE 125, 260 <312 f.>). 334

However, the authorisation permitting the Bavarian *Land* Office to access traffic data was not, and is not, mirrored by any provision allowing or obliging service providers to share data with the Bavarian *Land* Office. § 113c(1) no. 2 TKG (former version) merely permitted service providers to share data with public security authorities and did not make any mention of domestic intelligence services. […] 335

The fact that Art. 15(3) BayVSG authorises the Bavarian *Land* Office to access data that service providers, under federal law, are not permitted to share with the Bavarian *Land* Office makes the provision unconstitutional. The case of a data access provision under *Land* law being inconsistent with a data sharing provision under federal law does more than simply render Art. 15(3) BayVSG meaningless. Divergence between data access and data sharing provisions violates the principle of legal clarity, thereby creating a legal framework that is unconstitutional. Data access provisions only satisfy the principle of legal clarity if they are consistent with the limited purposes set out in the corresponding data sharing provisions (cf. BVerfGE 155, 119 <209 para. 200>). This is not the case here. 336

5. Art. 18(1) BayVSG – undercover officers

Art. 18 BayVSG governs the use of undercover officers, i.e. staff members of the Bavarian *Land* Office who operate under a cover given to them on a permanent basis. The provision violates the fundamental right to informational self-determination (Art. 2(1) in conjunction with Art. 1(1) GG) because it does not establish a sufficient threshold for interference, does not define the permissible targets of surveillance, and does not provide for (repeated) oversight by an independent body. 337

a) aa) Measures under Art. 18(1) BayVSG can interfere with the fundamental right to informational self-determination if undercover officers gain access to personal data during the course of their undercover activities. It does not constitute interference if undercover officers merely communicate with a target person while operating under their cover identity. However, it does constitute interference if undercover officers exploit the target person’s legitimate expectations regarding the identity and motivation of their communication partner in order to thereby gain access to personal data they would not otherwise have obtained (cf. on the use of an undercover identity when communicating online, BVerfGE 120, 274 <345> with further references; cf. on the use of undercover officers, BVerwG, Judgment of 29 April 1997 - 1 C 2/95 -, juris, para. 22; […]). In cases where undercover officers are used to investigate endeavours warranting surveillance, legitimate expectations of this nature are almost always exploited. Members of such endeavours or persons close to them would be extremely unlikely to share information with an undercover officer if the latter’s true identity were known. Personal information is often divulged in the process. If the information concerns a third party rather than a person actively involved in the endeavour, this must be regarded as constituting interference with the third party’s fundamental right to informational self-determination. 338

[…] 339

bb) The use of undercover officers can be extremely intrusive ([...]). It can involve cultivating and then exploiting what appears to be a genuine relationship of trust. This often means establishing and then exploiting a person’s trust in an undercover officer’s apparent motivation and identity. The entire point of such operations is to elicit information from a target person – someone who unsuspectingly places their trust in 340

an undercover officer or at least believes that the undercover officer's apparent identity is genuine and who subsequently reveals information they would not have disclosed if they were aware of the true circumstances. In cases where the state exploits personal trust in order to overcome a person's interest in maintaining secrecy, thereby inducing them to disclose information, the resulting interference can be extremely severe.

That being said, the severity of interference resulting from measures under Art. 18(1) BayVSG can vary considerably, the decisive factor being the specific nature of the measure in question. The severity depends in particular on the duration of an undercover officer's deployment and on how intense the relationships become, with the intensity of communication being significant in both quantitative and qualitative terms. One relevant factor here is the specific form of the interactions that take place between the undercover officer and the other members of the endeavour under surveillance. It makes a difference if undercover officers simply attend a general meeting once a month or if they are in intense contact with a small group of people on a daily basis. Another factor is whether the undercover assignment merely targets an organisation as a whole or is directed against a specific individual. Where an apparently genuine relationship of trust is cultivated to a deeper level, the resulting interference is particularly severe. The more intense the relationship becomes and the more information the target person reveals, the more profound is the interference with fundamental rights. The interference is also particularly severe if the measure is directed against persons who are not themselves part of the endeavour. 341

b) Art. 18(1) BayVSG is unconstitutional because the prerequisites for interference contained therein do not satisfy the constitutional requirements (see aa) below) and because it does not provide for *ex ante* oversight by an independent body (see bb) below). 342

aa) (1) The principle of proportionality in the strict sense requires that measures under Art. 18(1) BayVSG only be authorised if they are necessary in the individual case to investigate a specific activity or group that warrants surveillance by an intelligence service. The legislator must take account of the fact that measures under Art. 18(1) BayVSG can give rise to very severe interference with fundamental rights. The longer an undercover officer is deployed, the deeper the relationships of trust become and the greater the amount of private information that is obtained, the more urgently must the measure necessitate surveillance and the more valuable must the intelligence be that the measure promises to yield. The legislator may not leave the task of assessing the proportionality requirements entirely to the domestic intelligence service, but rather must itself define key criteria regarding the severity of interference on the one hand and the urgency of the measure on the other. The law must set out explicit requirements reflecting the fact that the interference grows increasingly severe the longer a measure continues, requiring a heightened need for surveillance and the promise of more valuable intelligence in order to justify the measure under constitutional law (see para. 192 ff. above for general details). In addressing this issue, the 343

legislator may provide for different thresholds depending on the severity of interference involved.

Art. 18(1) BayVSG does not satisfy the above requirements because it does not define its own thresholds for interference. Rather, the prerequisites for carrying out measures under Art. 18(1) BayVSG are derived from the general provisions set out in Art. 5(1) BayVSG. The second sentence of that provision requires factual indications of anti-constitutional endeavours or activities within the meaning of Art. 3 BayVSG. Pursuant to Art. 5(1) first sentence nos. 1 to 3 BayVSG, the measures must furthermore be necessary in order for the Bavarian *Land* Office to fulfil its tasks under Art. 3 BayVSG, or for investigating and assessing endeavours and activities as well as the intelligence sources necessary to monitor them, or for protecting the staff, facilities, equipment and intelligence sources of the Bavarian *Land* Office against intelligence service activities and activities that threaten public security. The law does not contain any further requirements as to the permissible duration of the use of undercover officers, nor does it require that the danger posed by the activities under surveillance be greater, the longer that undercover officers are deployed (cf. in this regard § 9a (1) second sentence BVerfSchG). This is not compatible with the constitutional requirements. 344

(2) Furthermore, the law does not limit the permissible targets of surveillance when the use of undercover officers is directed against specific persons. Neither Art. 18 BayVSG nor Art. 5 BayVSG contains any provision on the permissible targets of intelligence service action. 345

However, it is not objectionable under constitutional law that the Bavarian *Land* Office is permitted by Art. 8(1) third sentence BayVSG to exercise the powers under Art. 18 BayVSG even if this unavoidably results in third parties being affected. The fact that persons who are not targets of surveillance come into contact with undercover officers is unavoidable because the latter need to maintain their cover identity on a permanent basis. [...] 346

By contrast, the targeted inclusion of third parties in the surveillance measures of the domestic intelligence services is subject to strict limits arising from the principle of proportionality. The more a third party is deliberately included in an undercover officer's surveillance activities, the closer the relationship linking the third party to the activity or group under investigation must be (for general details, see para. 212 above). The legislator is obliged to set limits here, as has been done in Art. 19a(2) no. 2 BayVSG with regard to observation. No comparable provision exists for the use of undercover officers. 347

bb) Art. 18 BayVSG is also unconstitutional insofar as it fails to provide for any independent *ex ante* oversight. Such oversight is essential under constitutional law due to the severity of interference ([...]). It is true that the severity of interference resulting from the use of an undercover officer depends on the specific form of the deployment (see para. 340 f. above). Nevertheless, the use of state employees to gather informa- 348

tion while undercover, without the target persons ever being aware of the fact and without them having any possibility to defend themselves against such activity under the rule of law, has such an adverse impact on the fundamental right to informational self-determination that – unless the undercover operation is only brief and relationships of trust are unlikely to be established – there is a need for independent *ex ante* oversight by an external body (cf. BVerfGE 141, 220 <294 para. 174>). In the case of longer-term assignments, this oversight must be exercised repeatedly, especially since the constitutional standards that apply when deciding whether to continue a measure can change over time. In particular, the value of the intelligence that the measure is expected to yield may have to satisfy more demanding criteria (see paras. 198 and 206 above). The independent oversight must serve to ascertain whether the measure in question satisfies the prerequisites for interference which apply to the respective surveillance period – prerequisites which the legislator is required to specify in some detail (see para. 199 ff. above). Oversight does not need to be exercised repeatedly if the legislator restricts the use of undercover officers to sufficiently brief periods from the outset. But no such time limits are set out in Art. 18 BayVSG.

6. Art. 19(1) BayVSG – informants

Art. 19 BayVSG governs the use of informants, i.e. individuals who cooperate on a systematic and long-term basis with the Bavarian *Land* Office for the Protection of the Constitution without third parties being aware of the fact. The provision makes reference to the requirements set out in Art. 18 BayVSG. Like Art. 18(1) BayVSG, Art. 19(1) BayVSG violates the fundamental right to informational self-determination (Art. 2(1) in conjunction with Art. 1(1) GG) because it does not establish a sufficient threshold for interference, does not define the permissible targets of surveillance, and does not provide for *ex ante* oversight by an independent body. 349

a) Here again, the interference with fundamental rights stems from the informant exploiting a supposedly genuine relationship of trust in order to obtain information from another person that the informant would not otherwise have been able to obtain (see para. 338 above). The fact that the informant is not employed by the Bavarian *Land* Office and is not therefore a direct agent of state authority makes no difference in this respect. The state bears responsibility here because, pursuant to Art. 19(2) first sentence BayVSG, the decision to sign up an informant is made by the head of the Bavarian *Land* Office, the informants collaborate with the Bavarian *Land* Office, and they forward their obtained information to the Bavarian *Land* Office ([...]). 350

Here too, the severity of the resulting interference depends on the circumstances of the specific deployment. The interference may be relatively mild at first. During the phase when new informants are being recruited, their previous relationships of trust may not yet have been entirely undermined by their obligations to the state and they may not yet be passing on extensive information. Over the long term, however, the use of informants under Art. 19 BayVSG tends to be just as intrusive as the use of undercover officers under Art. 18 BayVSG. Relationships that were once genuinely 351

based on trust can be covertly and unilaterally subverted and transformed into relationships defined by surveillance.

b) In principle, therefore, the same constitutional requirements that apply to provisions governing the thresholds for interference and the permissible targets of surveillance when using undercover officers under Art. 18 BayVSG also apply when using informants under Art. 19 BayVSG. These requirements have not been met. 352

aa) Here too, the provision lacks a sufficient threshold for interference and there is no limitation of permissible targets of surveillance when the use of informants is directed against specific persons (see paras. 343 f. and 345 ff. above). On the other hand, the legislator is permitted to set thresholds for the use of informants that take account of the fact that the preparatory phase may need to be longer than when using undercover officers. [...] In principle, it is not therefore objectionable to provide for a recruitment and probationary phase that informants must complete before they are permanently signed up. [...] The legislator must ensure that the decision to sign up an informant is taken within a reasonable period of time. 353

bb) As with the use of undercover officers, (repeated) independent oversight is essential under constitutional law due to the severity of interference resulting from the use of informants under Art. 19(1) BayVSG (cf. BVerfGE 141, 220 <294 para. 174>; on undercover officers, see para. 348 above). As long as the legislator ensures that any recruitment and probationary phase which may be necessary for practical purposes is limited to a reasonable period (see para. 353 above), the constitutional requirements are satisfied if the oversight starts with the decision to actually sign up an informant. Here too, oversight must be exercised repeatedly unless the cooperation agreement is limited from the outset to a sufficiently brief period. Neither of these requirements are provided for in Art. 19 BayVSG. It is true that Art. 19(2) fourth sentence BayVSG does require the use of informants to be terminated after a maximum of six months if the measure has not sufficiently contributed to investigating a specifically defined endeavour. However, this only applies to special cases in which the person who was signed up as an informant was previously convicted of committing culpable homicide or a criminal offence only punishable by life imprisonment. 354

Given the particular risks especially to life and limb that informants can face if their identity is exposed, it is necessary under constitutional law – primarily on account of Art. 2(2) first sentence GG – to design the independent oversight process in a way that protects their fundamental rights (cf. BVerfGE 146, 1 <45 ff. para. 100 ff.>; 156, 270 <305 para. 108>). 355

7. Art. 19a(1) BayVSG – observation outside the home

Art. 19a(1) BayVSG authorises the Bavarian *Land* Office for the Protection of the Constitution to observe a person covertly and systematically outside the scope of Art. 13 GG, including by technical means, for longer than 48 hours or on more than three days within a week. The provision violates the fundamental right to informational self- 356

determination (Art. 2(1) in conjunction with Art. 1(1) GG) because it does not establish a sufficient threshold for interference and does not provide for (repeated) oversight by an independent body.

a) The long-term observation permitted by Art. 19a BayVSG interferes with the general right of personality under Art. 2(1) in conjunction with Art. 1(1) GG in its manifestation as a right to informational self-determination. The severity of interference resulting from observation measures can vary greatly, ranging from interferences of low to medium severity such as the taking of isolated photographs or simple observation for a limited period, to serious interferences such as long-term monitoring by means of covert audio and image recordings of a person. Particularly when these measures are combined with the aim of registering and audio-visually recording as many of the target person's statements and movements as possible with the help of technology, they can reach deep into the private sphere and thus constitute interferences of particular severity (cf. BVerfGE 141, 220 <287 para. 151>). Although these measures concern surveillance that, by definition, takes place outside the home, it is nonetheless likely that they will result in the recording of highly confidential situations – be it in the car, be it sitting away from the crowds in a restaurant, be it on a secluded stroll (cf. BVerfGE 141, 220 <295 para. 176>). 357

b) Art. 19a BayVSG does not entirely satisfy the constitutional requirements applicable to the long-term observation measures permitted thereunder. 358

aa) The principle of proportionality in the strict sense requires that measures under Art. 19a BayVSG only be authorised if they are necessary in the individual case to investigate a specific activity or group that warrants surveillance by an intelligence service. The decisive factor here is whether the intelligence sought by the measure has specific relevance for the further investigation of anti-constitutional endeavours. Since measures of this kind are usually directed against certain individuals, the surveillance of these precise individuals must contribute to the investigation. Furthermore, the provision authorising the measure must take account of the potentially considerable severity of the resulting interference, setting detailed requirements with regard to the need for surveillance of the observed endeavour and, at least for particularly intrusive measures, making the authorisation contingent upon a particularly heightened need for surveillance (on the requirements generally, see para. 192 ff. above). While the covert use of technical means for recording images would certainly fall into this latter category, a particularly heightened need for surveillance is not required for measures that result in interference of low to medium severity. The legislator is thus permitted to set thresholds with varying degrees of strictness for the observation powers under Art. 19a BayVSG, depending on the severity of interference in each case. If this is not done, the threshold must satisfy the constitutional requirements that apply to the severest possible level of interference. 359

Art. 19a BayVSG does not fully comply with these standards. It is true that Art. 19a(2) BayVSG does limit the permissible targets of surveillance in a manner that 360

satisfies the constitutional requirements. Furthermore, Art. 19a(1) last half-sentence BayVSG requires that observation measures only be authorised if they are necessary for the surveillance of endeavours or activities of considerable significance. Thus the law does require a heightened need for surveillance. However, the particularly heightened need for surveillance that is required in the case of especially intrusive long-term observation measures, and the basis for such need, are not sufficiently specified by requiring that endeavours or activities be of considerable significance. [...]

bb) Art. 19a(1) BayVSG is also unconstitutional insofar as it does not provide for independent *ex ante* oversight. Such oversight is necessary at least in the case of long-term observation measures that interfere profoundly with the fundamental rights of the persons concerned (cf. BVerfGE 141, 220 <294 para. 174> […]). The legislator must also impose time limits on long-term measures or provide for repeated oversight. However, the Basic Law does leave room for the legislator to enact special provisions that cover exceptional cases of danger requiring imminent action (cf. BVerfGE 141, 220 <302 para. 204>). 361

8. Art. 25 BayVSG – data sharing by the Bavarian Land Office for the Protection of the Constitution

Insofar as Art. 25 BayVSG is admissibly challenged, the data sharing powers set out therein do not satisfy the constitutional requirements (see para. 225 ff. above for general remarks). Of the numerous data sharing provisions contained in Art. 25 BayVSG, the complainants only object to the sharing of personal data and information collected using intelligence service methods. [...] Data sharing under Art. 25 BayVSG affects the general right of personality in its manifestation as a right to informational self-determination. 362

a) Art. 25(1) no. 1 second alternative BayVSG, which permits data sharing with domestic bodies “for other public security purposes”, does not establish sufficient statutory requirements for data sharing. 363

aa) Art. 25(1) no. 1 second alternative BayVSG does not satisfy the constitutional requirements regarding the legal interest to be protected by data sharing. The term “public security purposes” encompasses the integrity of the entire legal order. As such, any breach of the law could justify data sharing. Yet the sharing of personal data and information collected by the Bavarian *Land* Office using intelligence service methods is only permissible to protect an exceptionally significant public interest (see para. 238 ff. above). This requirement is lacking in Art. 25(1) no. 1 BayVSG. 364

[…] 365-367

bb) The provision furthermore lacks a threshold for data sharing as required under constitutional law. Art. 25(1) no. 1 second alternative BayVSG merely requires there to be factual indications that the recipient needs the information for public security purposes. The concept of “need” is an extremely broad criterion. Information may be “needed” well in advance of any danger to public security: to help an authority better 368

evaluate the overall situation, for example, or to enhance its ability to plan. This does not satisfy the constitutional requirements. It is true that data may be shared prior to any specific dangers arising, provided that the receiving body does not have operational powers. However, this condition is not guaranteed here. In any case, not even this would justify a general relaxation of the requirements that apply to sharing of data collected by an intelligence service (see para. 259 above).

b) Art. 25(1) no. 3 BayVSG is likewise unconstitutional. It authorises the Bavarian *Land* Office to share information, including personal data, with any domestic public body – even if the information was collected using intelligence service methods – if there are factual indications that the recipient needs the information for the performance of its assigned duties, provided that the recipient is thereby also acting for the protection of the free democratic basic order or must assess issues of public security or Germany's foreign interests. 369

aa) It is true that in designating the free democratic basic order as a legal interest to be protected, the legislator has named a legal interest of sufficient weight. However, the provision merely requires that the recipient need the information for the performance of its assigned duties, provided that the recipient is thereby "also" acting for the protection of the free democratic basic order. This means that data sharing is allowed practically without restriction because virtually every authority is called upon to protect this interest [...]. [...] 370

bb) Art. 25(1) no. 3 BayVSG does not establish sufficient thresholds for data sharing. Once again, the provision merely requires the presence of factual indications that the recipient needs the information. This does not satisfy the constitutional requirements (see para. 368 above). 371

c) Art. 25(1a) BayVSG governs the sharing of data by the Bavarian *Land* Office with public and non-public bodies in other European states. The provision is admissibly challenged only insofar as it concerns the sharing of data with public bodies. This aspect does not satisfy the constitutional requirements. Because Art. 25(1a) BayVSG refers to Art. 25(1) BayVSG without restriction, it shares the same constitutional deficiencies as that provision. These deficiencies are exacerbated by the fact that Art. 25(1a) BayVSG allows data collected using intelligence service methods to be shared with security authorities with operational powers in other European states under the lenient conditions of Art. 25(1) BayVSG; by contrast, the sharing of such data with the equivalent domestic authorities is subject to the stricter requirements of Art. 25(2) BayVSG. The Bavarian *Land* Government submits that the principle of separation of police and intelligence data (*informationelles Trennungsprinzip*) may be an unfamiliar concept in other EU Member States. In such cases, data may only be shared for public security or prosecution purposes if there is at least an identifiable danger to a particularly weighty legal interest or if there is sufficient suspicion that a particularly serious criminal act has been committed (see paras. 235 ff. and 249 ff. above). 372

d) Art. 25(2) first sentence BayVSG authorises data sharing with authorities that 373

have executive powers. Art. 25(2) first sentence no. 2 BayVSG authorises data sharing for the purpose of averting, preventing or prosecuting considerable criminal offences. For all three alternatives, the authorisation falls short of the constitutional requirements (see paras. 235 ff. and 249 ff. above). The same applies for Art. 25(2) first sentence no. 3 BayVSG.

aa) In formulating the provisions authorising the sharing of data for the purpose of averting or preventing considerable criminal offences under Art. 25(2) first sentence no. 2 first and second alternatives BayVSG, the legislator has not named a legal interest of sufficient weight. Data sharing for public security purposes must serve to protect an exceptionally significant public interest. This is equivalent to limiting the sharing of data to cases involving particularly serious criminal offences (see paras. 236 ff. and 251 above). 374

Furthermore, the provision does not establish a sufficient threshold for data sharing. Data originally collected by a domestic intelligence service may only be shared with a public security authority if there is a specific or identifiable danger (see para. 245 ff. above). Yet the law allows such data to be shared for the general purpose of preventing considerable criminal offences. Since it places no specific limits on the permissible grounds for data sharing, the law allows information to be shared with a police authority purely on the basis of the information's potential value in providing leads for further investigations (cf. BVerfGE 141, 220 <336 f. para. 313>). This does not satisfy the constitutional requirements. 375

When revising the data sharing threshold, the legislator must take care not to formulate permissible grounds that would enable data to be shared long before any dangers to the designated legal interests have emerged in recognisable detail. Given the severity of the resulting interference, shifting the threshold for data sharing to a purely precautionary stage is incompatible with the Constitution if it means that such measures could be carried out on grounds of vague indications of possible dangers (cf. BVerfGE 141, 220 <273 para. 113>; cf. BVerfGE 100, 313 <395>). 376

bb) In formulating the provision authorising the sharing of data for the purpose of prosecuting considerable criminal offences under Art. 25(2) first sentence no. 2 third alternative BayVSG, the legislator has again failed to name a legal interest that meets the applicable requirements. Domestic intelligence services are only permitted to share data originally collected by them with prosecution authorities for the purpose of prosecuting criminal offences that are particularly serious. Criminal offences that are merely considerable are not sufficient in this regard (see para. 251 above). 377

cc) Art. 25(2) first sentence no. 3 BayVSG likewise fails to establish sufficient requirements for data sharing. The provision simply refers to the fact that the recipient needs to have powers that would have enabled it to directly collect the information itself. However, a provision that allows the sharing of data for purposes other than those originally envisaged must itself state these other purposes in a manner that is in conformity with the Constitution (cf. BverfGE 130, 1 <34>). 378

e) Art. 25(3) first sentence no. 2 BayVSG, which authorises data sharing with foreign public bodies, as well as supranational and international bodies, likewise fails to satisfy the constitutional requirements. By allowing data sharing where mere factual indications exist that the sharing of data is necessary to protect the recipient's significant security interests, the legislator has not defined the permissible grounds for data sharing with sufficient specificity under constitutional law. 379

The same constitutional requirements for sharing data that was originally collected by an intelligence service with bodies in Germany also apply to the sharing of intelligence service data with other states (see para. 261 above). Thus, such data may only be shared for the purpose of protecting an exceptionally significant public interest, and the law must be sufficiently specific in setting out the permissible grounds, i.e. in defining the threshold for data sharing (see para. 261 ff. above). Yet here, the law fails to establish a threshold for data sharing as required under constitutional law. It permits data sharing where mere factual indications exist that the sharing of data is necessary to protect the recipient's significant security interests. This fails to set forth specific grounds for investigation, either in the context of police investigation or intelligence service work. Making the permissibility of data sharing contingent upon its "necessity" is not sufficient (cf. BVerfGE 154, 152 <306 para. 314>). 380

9. Art. 8b(2) first sentence no. 2 BayVSG – data originating from the surveillance of private homes and remote searches

Art. 8b(2) BayVSG governs the processing of data originating from the surveillance of private homes (Art. 9(1) BayVSG) and remote searches (Art. 10(1) BayVSG). Like the interference resulting from the original data collection, interferences stemming from any sharing or processing of data that changes the original purpose must be measured against Art. 13 GG and the general right of personality in its manifestation as a right to the confidentiality and integrity of information technology systems. 381

Ultimately, the reference in Art. 8b(2) BayVSG to § 100b(2) StPO is unconstitutional. It must be assumed that the reference cites whichever version of § 100b(2) StPO is currently effective at the time, making it a so-called dynamic statutory reference. The legislative materials likewise suggest that the legislator deliberately intended to use a dynamic reference (cf. BayLTDrucks 17/11609, p. 18). The constitutional requirements applicable to dynamic references (see a) below) are not satisfied in this case (see b) below). 382

a) If a legislator regulates a subject matter using a dynamic statutory reference, special constitutional requirements apply. 383

Laws do not necessarily have to set out every single aspect of the relevant statutory requirements themselves. Rather, they can make reference to other provisions. References to provisions enacted by other legislative authorities are not impermissible in principle (cf. BVerfGE 26, 338 <366 f.>; 29, 198 <210>; 47, 285 <312>; 141, 143 <176 f. para. 75>). References are constitutionally unobjectionable if the legislator 384

making the reference adopts the substance of another legislative authority's statutory provisions using a so-called static reference that refers to the version in effect at the time when the legislation was enacted (cf. BVerfGE 47, 285 <312>; 141, 143 <176 f. para. 75>; 153, 310 <342 para. 79> with further references – Cartilage in meat […]).

With dynamic statutory references, the situation is somewhat different. While they are not impermissible per se, stricter requirements apply. Dynamic references to provisions enacted by other legislative authorities are only permissible within the boundaries set by the principles of the rule of law and democracy in particular (cf. BVerfGE 141, 143 <176 f. para. 75>; 143, 38 <62 para. 59>; 153, 310 <343 para. 79>; established case-law). The main limiting factor on the permissibility of dynamic references is the requirement that interferences with fundamental rights be based on a statutory provision (cf. BVerfGE 47, 285 <312 ff.>; 78, 32 <36>; 143, 38 <56 para. 43, 62 para. 59>; 153, 310 <343 f. para. 79>; […]). Laws that authorise interference with a fundamental right must strike a balance between the fundamental right at issue, other conflicting fundamental rights, other constitutional interests and any other protected interests. If a legislator creates powers that interfere with fundamental rights, it is obliged to conduct a balancing of the affected fundamental rights. It thereby assumes accountability for the resulting decision on how that balancing is to be achieved. But if a *Land* legislator makes a dynamic reference to a federal law, the chain of accountability becomes problematic. The danger here is that no legislative authority will then be fully accountable for the necessary decision on how the different interests should be balanced. The federal legislator has no reason to consider what impact its legislation might have on *Land* law and on the balancing of interests necessary within *Land* law, nor is it in principle under any obligation to do so. For its part, a *Land* legislator cannot properly balance the different interests involved if it is unable to conclusively assess the overall situation due to the dynamic nature of the law being referred to. It may nonetheless be permissible for a *Land* law to make a dynamic reference to a federal law in cases where the referenced provisions relate to a narrowly defined field and their contents are already essentially certain (cf. BVerfGE 23, 265 <269 f.>; 26, 338 <366 f.>; 153, 310 <343 para. 79>). 385

b) Art. 8b(2) first sentence no. 2 BayVSG does not satisfy the constitutional requirements for dynamic statutory references. The provision grants authorisation for the processing, including the sharing, of data originating from the surveillance of private homes and remote searches. These are separate and particularly intrusive interferences with fundamental rights. As such, they must be based on statutory provisions that set out the requirements for the processing and sharing of data. This was not done here in the required manner. Rather, by making a dynamic reference to § 100b(2) StPO, the Bavarian legislator adopted the federal legislator's assessment with regard to the type of criminal acts whose potential or actual commission would justify the processing and sharing of data – an assessment capable of changing over time in ways the *Land* legislator is unable to predict, and which the *Land* legislator cannot therefore rely upon when carrying out the balancing of fundamental rights for 386

which it is responsible. Furthermore, § 100b(2) StPO cannot be described as concerning a narrowly defined field, the contents of which are largely certain. Security law – including provisions under criminal procedural law that confer investigatory powers, such as § 100b StPO, along with the offences referred to therein – is subject to considerable changes. [...] In political terms, security law is a highly contested field. It is hard to predict how the federal investigatory powers set out in § 100b StPO might be amended in future.

A restrictive interpretation in conformity with the Constitution is not possible. [...] 387

[…] 388

10. Art. 8b(3) BayVSG – data from requests for information

Art. 8b(3) BayVSG concerns the internal processing within the Bavarian *Land* Office of personal data obtained from measures under Art. 15(2) and (3) and Art. 16(1) BayVSG as well as the sharing of such data with other bodies. Like the interference resulting from the original data collection, interferences stemming from any sharing or processing of data that changes the original purpose must be measured against the general right of personality in its manifestation as a right to the confidentiality and integrity of information technology systems, and also to some extent against [the privacy of telecommunications under] Art. 10(1) GG. The dynamic reference in Art. 8b(3) BayVSG that refers to § 4(4) first sentence nos. 1 and 2 G 10 is incompatible with the constitutional requirements […]. The multi-link chains of statutory references furthermore violate the principle of legal clarity [...]. 389

[…]

D. Outcome and legal consequences

I.

Ultimately, the provisions that were admissibly challenged do not entirely satisfy the constitutional requirements. In this respect, the constitutional complaint is for the most part well-founded. 392

1. Art. 9(1) first sentence BayVSG [*surveillance of private homes*] is unconstitutional. Although the powers conferred thereunder do in principle require sufficient prerequisites (“acute danger”) for carrying out surveillance measures which constitute interferences with fundamental rights, the provision is not aimed at the purpose of averting such danger. The provision also lacks the necessary element of subsidiarity vis-à-vis public security measures taken by public security authorities. Moreover, the constitutional requirements for protecting the core of private life applicable to the surveillance of private homes are not fully met, either at the data collection stage or the data analysis stage. 393

Art. 10(1) BayVSG [*remote searches*] is unconstitutional because, by making reference to Art. 9(1) BayVSG, it shares the same constitutional deficiencies as that pro- 394

vision. Although it meets the constitutional requirements for protecting the core of private life at the data collection stage, it is deficient with respect to the data analysis stage.

Art. 12(1) BayVSG [*tracking of mobile devices*] is unconstitutional because the authorisation allows for the long-term monitoring of the movements of affected persons, without containing sufficiently specific prerequisites for interference. Moreover, the required independent *ex ante* oversight is lacking. 395

Art. 15(3) BayVSG [*disclosure of traffic data originating from data retention*] is incompatible with the principle of legal clarity – the only standard against which this provision was reviewed. 396

Art. 18(1) and Art. 19(1) BayVSG [*undercover officers*; *informants*] are unconstitutional because they do not provide a sufficient threshold for interference and there is no restriction on the scope of permissible targets of surveillance if the use of undercover officers or informants is directed at specific persons. Moreover, there is a lack of independent *ex ante* oversight. 397

Art. 19a(1) BayVSG [*observation outside the home*] is unconstitutional because in the case of particularly intrusive observation measures, the authorisation is not limited to anti-constitutional endeavours or activities that particularly warrant surveillance. Furthermore, there is also a lack of independent *ex ante* oversight. 398

2. Insofar as the data sharing provisions of Art. 25 BayVSG were admissibly challenged, they do not satisfy the constitutional requirements. This applies to Art. 25(1) no. 1 second alternative, Art. 25(1) no. 3, Art. 25(1a), Art. 25(2) first sentence nos. 2 and 3 and Art. 25(3) first sentence no. 2 BayVSG. 399

The powers of data processing and sharing under Art. 8b(2) first sentence no. 2 BayVSG are unconstitutional in terms of their specific legislative design due to the impermissible dynamic reference to federal law. This also applies to Art. 8b(3) BayVSG. Furthermore, the multi-level chains of statutory references contained in this provision violate the principle of legal clarity. 400

II.

1. The finding that a statutory provision is unconstitutional generally results in that provision being declared void. However, pursuant to § 31(2) second and third sentence BVerfGG, the Federal Constitutional Court can limit its decision to declaring that an unconstitutional provision is merely incompatible with the Constitution. It then merely objects to the unconstitutional provision without declaring it void. The Court may combine the declaration of incompatibility with a temporary order to continue to apply the unconstitutional provisions. This may be considered in cases where the immediate invalidity of the objectionable provision would eliminate the statutory basis for protecting exceptionally significant interests of the common good, and if a balancing of these interests against the affected fundamental rights requires that the inter- 401

ference be tolerated for a transitional period. During the transitional period, the Federal Constitutional Court can issue interim orders to reduce the powers of the authorities, in line with what appears necessary in light of its balancing, until a situation of constitutional conformity has been established (BVerfGE 141, 220 <351 para. 355> with further references; established case-law).

2. a) In light of the above, Art. 15(3) BayVSG is declared unconstitutional and void. This provision does not satisfy the constitutional requirements and the *Land* legislator cannot remedy this by adopting a constitutionally compatible provision with comparable legislative content. 402

b) By contrast, the following provisions are merely declared incompatible with the Constitution: Art. 9(1) first sentence, Art. 10(1), Art. 12(1), Art. 18(1), Art. 19(1) and Art. 19a(1) BayVSG, as well as Art. 8b(2) first sentence no. 2, Art. 8b(3), Art. 25(1) no. 1 second alternative, Art. 25(1) no. 3, Art. 25(1a), Art. 25(2) first sentence nos. 2 and 3, and Art. 25(3) first sentence no. 2 BayVSG. The declaration that the provisions are incompatible with the Constitution is combined with the order that they are nonetheless to stay in effect on an interim basis until 31 July 2023 at the latest. The grounds for the unconstitutionality of the provisions do not affect the core of the powers granted through the provisions but merely touch upon individual aspects of their design in light of the rule of law. Under such circumstances, the legislator is given the opportunity to remedy the constitutional concerns and thereby achieve the core of the objectives pursued by the provisions. Given the great importance of having an effective domestic intelligence service for the purposes of maintaining a free and democratic state based on the rule of law, the provisions' continued interim applicability is more tolerable than a declaration of their voidness; a declaration to that effect would deprive the Bavarian *Land* Office for the Protection of the Constitution of pivotal investigatory powers until the adoption of new legislation (cf. BVerfGE 141, 220 <352 para. 357>). 403

c) However, in ordering the continued applicability of the provisions, it is necessary to impose certain restrictions to protect the affected fundamental rights. First, it is ordered that measures pursuant to Art. 9(1) first sentence and Art. 10(1) BayVSG [*surveillance of private homes; remote searches*] are only to be taken for the purpose of averting the type of dangers required in those cases, and then only in the event that suitable police assistance for the legal interest at risk cannot otherwise be timely obtained. In this respect, Art. 8a(1) BayVSG must be applied subject to the rebuttable presumption that intelligence obtained from the surveillance of a private home concerns the core of private life. 404

Second, it is ordered that technical means are not to be deployed under Art. 12(1) BayVSG [*tracking of mobile devices*] in such a way that the movements of a mobile device belonging to a person under surveillance are tracked over a prolonged period. 405

Furthermore, the use of undercover officers under Art. 18(1) BayVSG and the use of informants under Art. 19(1) BayVSG must be terminated after a maximum of six 406

months if such use is not essential for investigating an endeavour aimed at the commission of particularly serious criminal acts which endanger the legal interests protected under § 3 BVerfSchG. If the use of undercover officers or informants is specifically directed against a certain person, then – applying Art. 19a(2) BayVSG accordingly – that person may only be someone who can be assumed, on the basis of factual indications, to be directly involved in the endeavour or activity, or – if a measure targeting such a person is insufficient on its own to establish the facts of the case – someone who is in contact with that person and has knowledge of the endeavour or activity or upon whom that person relies to support the endeavour or activity. Technical means may be used covertly under Art. 19a(1) BayVSG [*observation outside the home*] to record images and to intercept and record non-public spoken communication only if this is essential for the investigation of an endeavour aimed at committing particularly serious criminal acts which threaten the legal interests protected under § 3 BVerfSchG and if the other statutory requirements are satisfied. Finally, the sharing under Art. 25 BayVSG of personal data and information obtained using intelligence service methods is only permissible to protect an exceptionally significant public interest. This is equivalent to limiting the sharing of such data to cases involving particularly serious criminal offences. Furthermore, the specific grounds for sharing the data must satisfy the applicable requirements (thresholds for data sharing) as set forth in the reasons of this judgment.

[…] 407

Harbarth Paulus Baer

Britz Ott Christ

Radtke Härtel

Bundesverfassungsgericht, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17

Zitiervorschlag BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 - Rn. (1 - 407), http://www.bverfg.de/e/rs20220426_1bvr161917en.html

ECLI ECLI:DE:BVerfG:2022:rs20220426.1bvr161917