Headnotes

to the Judgment of the First Senate of 20 April 2016

1 BvR 966/09, 1 BvR 1140/09

1. **a) The authorisation of the Federal Criminal Police Office to carry out covert surveillance measures (surveillance of private homes, remote searches of information technology systems, telecommunications surveillance, collection of telecommunications traffic data and surveillance outside of private homes using special means of data collection) is, for the purpose of averting dangers to public security posed by international terrorism, in principle compatible with the fundamental rights enshrined in the Basic Law.**

   b) The design of these surveillance powers must satisfy the principle of proportionality. Powers that reach deep into private life must be limited to the protection or defence of sufficiently weighty legal interests; require the existence of a sufficiently specific and foreseeable danger to these interests; ensure that extending the measures to third parties who belong to the target person's contacts but are not themselves legally responsible for the danger is only permissible subject to very restrictive conditions; must be supplemented, for the most part, by specific provisions for the protection of the core of private life as well as the protection of persons bound by professional confidentiality; are subject to requirements of transparency, individual legal protection and administrative oversight; and must be supplemented by deletion requirements regarding the collected data.

2. **The constitutional requirements for the use and sharing of data collected by the state are informed by the principles of purpose limitation and change in purpose.**

3. **The scope of a purpose limitation depends on the respective statutory basis for the data collection measure in question: the initial purpose of data collection measures is limited to the respective investigation.**

4. **The legislator may permit data use beyond the specific investigation that prompted the data collection measure if the envisaged data use is still in line with the purpose for which the data was originally collected (further use). This requires that the use of collected data be limited to the same authority performing the same task and protecting the same legal interests. For data obtained through the surveillance of private homes or through remote searches of information technology systems, any further use must additionally satisfy the prerequisites for establishing sufficient indications of an identifiable danger that were applicable to the original data collection.**

5. **In addition, the legislator may also permit further use of collected data for purposes other than those for which the data was originally collected (change in purpose).**

   The proportionality requirements applicable to such a change in purpose derive from the principle of a hypothetical recollection of data. According to this principle, the new use of the data must serve to protect legal interests or to detect criminal acts of such weight that would, by constitutional standards, justify a new collection of the data by means entailing interferences that are comparable in severity [to the original data collection measures]. However, there is generally no need to establish, for a second time, the existence of an identifiable danger, as required for the original data collection; it is necessary but generally also sufficient to require that there be a specific basis for further investigations.

   With regard to data obtained through the surveillance of private homes and through remote searches of information technology systems, a change in purpose is only permissible if the prerequisites for establishing sufficient indications of danger that were applicable to the original data collection would also be satisfied in relation to the new purpose.

   The sharing of data with foreign state authorities is subject to the general constitutional principles of purpose limitation and change in purpose. In this context, the assessment of new data uses must respect the autonomy of the foreign state's legal order. Moreover, it must be ensured that the receiving state will handle the data in accordance with the rule of law.

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 966/09 -

- 1 BvR 1140/09 -

IN THE NAME OF THE PEOPLE

**In the proceedings
on the constitutional complaints of**

1. Mr B…, 2. Mr F…, 3. Mr S…, 4. Prof. Dr. H…, 5. Dr. N…, 6. Mr H…,

– authorised representatives: …

against § 14, § 20c(3), § 20g, § 20h, § 20k, § 20l, § 20u(1) and (2), § 20v and § 20w of the Federal Criminal Police Office Act in the version of 31 December 2008 (BGBl 2008, p. 3083 *seq*.)

- 1 BvR 966/09 -,

2. Mr W…, 2. Mr S…, 3. Dr. T…, 4. Ms R…, 5. Mr N…, 6. Mr T…, 7. Ms M…, 8. Ms K…, 9. Mr B…,

– authorised representative: …

against a) § 20g(1) and (2), § 20h(1), (2) and (5), § 20j(1), § 20k(1) and (7), § 20l(1) and (6), § 20m(1), § 20v(4) second sentence and (6) fifth sentence,
§ 20w(2) first and second sentence of the Federal Criminal Police Office Act,

b) § 20h(5) tenth sentence, § 20k(7) eighth sentence,
§ 20l(6) tenth sentence of the Federal Criminal Police Office Act,

c) § 20u(1) and (2) of the Federal Criminal Police Office Act in conjunction with
§ 53(1) first sentence nos. 2 and 3 of the Code of Criminal Procedure

- 1 BvR 1140/09 -

the Federal Constitutional Court – First Senate –

with the participation of Justices

Vice-President Kirchhof,

Gaier,

Eichberger,

Schluckebier,

Masing,

Paulus,

Baer,

Britz

held on the basis of the oral hearing of 7 July 2015:

JUDGMENT

1. **§ 20h(1) no. 1 lit. c of the Federal Criminal Police Office Act as amended by the Act on the Averting of Dangers from International Terrorism by the Federal Criminal Police Office of 25 December 2008 (BGBl I, p. 3083), and in the later amended versions, violates Article 13(1) of the Basic Law and is void.**

2. **§ 20v(6) fifth sentence of the Federal Criminal Police Office Act violates Article 2(1) in conjunction with Article 1(1), Article 10(1), Article 13(1), each in conjunction with Article 19(4) of the Basic Law, and is void.**

3. **§ 14(1) (excluding first sentence no. 2), § 20g(1) to (3), §§ 20h, 20j, 20k, 20l, § 20m(1) and (3), § 20u(1) and (2), and § 20v(4) second sentence, §20v(5) first to fourth sentence (excluding third sentence no. 2), § 20v(6) third sentence of the Federal Criminal Police Office Act are not compatible with Article 2(1) in conjunction with Article 1(1), Article 10(1), Article 13(1) and (3) – also in conjunction with Article 1(1) and Article 19(4) of the Basic Law – as set forth in the reasons of this judgment.**

4. **Until the legislator has enacted new provisions, or until 30 June 2018 at the latest, the provisions that have been declared incompatible with the Basic Law continue to apply, subject to the condition that measures pursuant to § 20g(2) nos. 1, 2 lit. b, 4 and 5 of the Federal Criminal Police Office Act require prior judicial authorisation; in cases of danger requiring immediate action, § 20g(3) second to fourth sentence of the Federal Criminal Police Office Act applies accordingly.**

Measures pursuant to § 20g(1) first sentence no. 2, § 20l(1) first sentence no. 2 and § 20m(1) no. 2 of the Federal Criminal Police Office Act may only be ordered if the prerequisites set out in § 20k(1) second sentence of the Federal Criminal Police Office Act, in the interpretation in conformity with the Basic Law as set forth in the reasons of this judgment, are fulfilled.

Further data use pursuant to § 20v(4) second sentence of the Federal Criminal Police Office Act or data sharing pursuant to § 20v(5) and § 14(1) of the Federal Criminal Police Office Act is permissible only in cases of acute danger where data obtained through the surveillance of private homes is concerned (§ 20h of the Federal Criminal Police Office Act); and only in cases of a specific impending danger to the protected legal interests where data obtained through remote searches of information technology systems is concerned (§ 20k of the Federal Criminal Police Office Act).

5. **[…]**

6. **For the rest, the constitutional complaints are rejected as unfounded.**

7. **[…]**

REASONS:

A.

I.

The constitutional complaints are directed against provisions of the Federal Criminal Police Office Act inserted […] by the Act on the Averting of Dangers from International Terrorism by the Federal Criminal Police Office of 25 December 2008 (BGBl I, p. 3083), effective 1 January 2009. On the basis of Art. 73(1) no. 9a of the Basic Law (BGBl I, p. 2034), as amended in 2006 with this purpose in mind, the federal legislator extended the existing mandate of the Federal Criminal Police Office in the domain of law enforcement by assigning it new tasks in the domain of averting dangers to public security posed by international terrorism, a responsibility that had until then been within the exclusive competence of the *Länder*. The constitutional complaints also challenge a provision in the Federal Criminal Police Office Act that predates the amendment at issue and concerns the sharing of data with foreign state authorities, the scope of which has been extended by the newly attributed tasks. 1

II.

Firstly, the constitutional complaints are directed against various investigatory powers conferred [upon the Federal Criminal Police Office]. The challenged powers include the authorisation to question persons pursuant to § 20c of the Federal Criminal 2

Police Office Act, as well as the use of special means of data collection outside of private homes pursuant to § 20g(1) to (3) of the Federal Criminal Police Office Act including, in particular, the covert interception and recording of non-public communication, covert image recording, the installation of tracking devices, and the use of police informants and undercover police investigators. The constitutional complaints also challenge the powers to carry out visual and acoustic surveillance of private homes pursuant to § 20h of the Federal Criminal Police Office Act, to conduct electronic profiling and searches pursuant to § 20j of the Federal Criminal Police Office Act, to access information technology systems pursuant to § 20k of the Federal Criminal Police Office Act, to monitor ongoing telecommunications pursuant to § 20l of the Federal Criminal Police Office Act as well as to collect telecommunications traffic data pursuant to § 20m(1) and (3) of the Federal Criminal Police Office Act. To that extent, the constitutional complaints also challenge § 20u of the Federal Criminal Police Office Act, which governs the protection of persons entitled to refuse to give evidence, as well as § 20w of the Federal Criminal Police Office Act, which sets out the requirement to notify affected persons after the surveillance measure has ended.

Secondly, the constitutional complaints are directed against provisions on data use. This concerns the use of data collected by the Federal Criminal Police Office itself […] pursuant to § 20v(4) second sentence of the Federal Criminal Police Office Act. They also challenge the power pursuant to § 20v(5) of the Federal Criminal Police Office Act – with the exception of third sentence no. 2 – to share this data with other domestic public authorities. Finally, the constitutional complaints also challenge § 14(1) first sentence nos. 1 and 3 and second sentence, § 14(7) of the Federal Criminal Police Office Act, which generally permits the sharing of data with foreign state authorities. By contrast, the present proceedings do not concern § 14a of the Federal Criminal Police Office Act, which additionally establishes special powers to share personal data with EU Member States. 3

[…] 4

III.

The complainants in proceedings 1 BvR 966/09 are lawyers, journalists, a doctor and a psychologist, most of whom are active in the field of human rights policy. The complainants in proceedings 1 BvR 1140/09 are former and current members of the German *Bundestag* – acting here as private individuals –, most of whom are also active in the human rights sector and some of whom also work as lawyers or doctors. In substance, they claim a violation of Art. 2(1) in conjunction with Art. 1(1), Art. 3(1), Art. 5(1) second sentence, Art. 10, Art. 12, Art. 13, in part also in conjunction with Art. 1(1), Art. 19(4) of the Basic Law and Art. 20(3) of the Basic Law. 5

[…] 6-40

IV.

[…] 41-73

V.

[…] 74

B.

The constitutional complaints are for the most part admissible. 75

I.

The constitutional complaints are directed against the surveillance and investigatory powers of the Federal Criminal Police Office, including in particular challenges to the inadequate protection of the core of private life and to the surveillance of persons entitled to refuse to give evidence, as well as against provisions on data use. […] 76

II.

[…] 77-78

III.

[…] 79-85

C.

To the extent that the constitutional complaints are directed against the investigatory and surveillance powers, they are well-founded in several respects. 86

I.

[…] 87-89

II.

The challenged surveillance and investigatory powers authorise interferences with fundamental rights, which, depending on the respective fundamental right and the differing weight of interference, must be measured individually against the principle of proportionality and the principle of legal clarity and specificity. The powers have in common that the potential interferences they authorise are for the most part serious. At the same time, since their purpose is to avert dangers to public security posed by international terrorism, they have a legitimate aim and are suitable and necessary for achieving that aim. 90

1. The challenged powers authorise the Federal Criminal Police Office to covertly collect personal data for the purposes of averting dangers to public security and of 91

preventing crime. Depending on the power in question, the measures result in interferences with the fundamental rights under Art. 13(1), Art. 10(1) and Art. 2(1) in conjunction with Art. 1(1) of the Basic Law, the latter both in its manifestation as the right to protection of the confidentiality and integrity of information technology systems and as the right to informational self-determination.

All these authorisations provide statutory bases for investigatory and surveillance measures that are usually carried out covertly without the knowledge of affected persons and can constitute deep intrusions into the private sphere. It is true that the challenged powers affect legitimate expectations of confidentiality to differing degrees and that the weight of interference varies significantly depending on the power in question. Yet the interferences they give rise to weigh heavily in any case, with the exception of certain measures set out in § 20g(1) and (2) of the Federal Criminal Police Office Act. 92

2. The constitutionality of the powers at issue depends on the limits arising from the different fundamental rights affected by them and the requirements deriving from the principle of proportionality, which must be determined individually for each of the powers in question. According to the principle of proportionality, the powers must in any case serve a legitimate aim and be suitable, necessary and proportionate in the strict sense for achieving this aim (cf. BVerfGE 67, 157 <173>; 70, 278 <286>; 104, 337 <347 *et seq*.>; 120, 274 <318 and 319>; 125, 260 <316>; established case-law). 93

Furthermore, the challenged powers must be measured against the principle of legal clarity and specificity, which serves to make interferences foreseeable for citizens, to effectively limit public authorities' powers and to enable effective judicial review (cf. BVerfGE 113, 348 <375 *et seq*.>; 120, 378 <407 and 408>; 133, 277 <336 para. 140>; established case-law). With regard to the powers at issue, which concern the covert collection and processing of data and can constitute a deep intrusion into the private sphere, this principle sets particularly strict requirements. […] 94

3. The challenged provisions pursue a legitimate aim and are suitable and necessary for achieving that aim. 95

a) The powers serve a legitimate aim. They provide the Federal Criminal Police Office with means of gathering information that it can use in fulfilling its new task of averting dangers to public security from international terrorism. The term 'international terrorism' is limited to specifically defined criminal offences of particular weight by means of the description of tasks laid down in § 4a(1) of the Federal Criminal Police Office Act and by means of that provision's reference to § 129a(1) and (2) of the Criminal Code, in line with the EU Framework Decision of 13 June 2002 and international terminology (OJ L 164, p. 3; Draft Comprehensive Convention on International Terrorism, in: Measures to eliminate international terrorism, Report of the Working Group of 3 November 2010, UN Doc. A/C.6/65/L.10) and in keeping with the Constitution-amending legislator's intent underpinning the insertion of Art. 73(1) no. 9a into the Basic Law (cf. BTDrucks 16/813, p. 12). Criminal offences characterised as ter- 96

rorism in this sense aim to destabilise society and, to this end, comprise attacks on the life and limb of random third parties, in a ruthless instrumentalisation of others. They are directed against the pillars of the constitutional order and society as a whole. Providing effective means of gathering information for averting terrorist dangers constitutes a legitimate aim and is of great significance for the free democratic order (cf. BVerfGE 115, 320 <357 and 358>; 120, 274 <319>; 133, 277 <333 and 334 para. 133>).

b) The surveillance and investigatory powers in question are suitable for achieving this aim. They provide the Federal Criminal Police Office with the means for gathering information that can be conducive to countering dangers posed by international terrorism. The different powers are, at least in principle, necessary for this task. Each of the powers in question allows the use of specific measures that cannot be replaced by alternative measures, at least not in every case. It is not ascertainable that there were less restrictive means that could provide equally effective and far-reaching possibilities of gathering information for averting dangers posed by international terrorism. At the same time, it must be ensured, in each individual case, that these powers only be exercised in accordance with the principle of suitability and necessity. 97

III.

The powers at issue must be sufficiently restricted in accordance with the principle of proportionality in the strict sense. This requires that the surveillance and investigatory powers in question be appropriate to their weight of interference. It is incumbent upon the legislator to balance the severity of the relevant interferences with fundamental rights of potentially affected persons, on the one hand, against the state's duty of protection regarding citizens' fundamental rights, on the other. 98

1. On the one hand, the legislator must take into account the weight of interference of the powers conferred by the challenged provisions. To differing degrees, depending on the power in question, these allow for far-reaching interferences with the private sphere and can, in individual cases, even intrude upon private refuges, the protection of which is of particular significance for safeguarding human dignity. In its balancing, the legislator must also consider developments in information technology, which increasingly extend the reach of surveillance measures, facilitate their use and enable the linking of data, which can go so far as to create personality profiles. In this regard, the constitutional assessment must distinguish between the different powers as well as the affected fundamental rights. 99

2. On the other hand, the legislator must ensure the effective protection of [other] fundamental rights and legal interests of citizens. In the constitutional assessment of appropriateness, it must be taken into account that the constitutional order, the existence and security of the Federation and of the *Länder*, and life, limb and liberty of the person are protected legal interests of significant constitutional weight. Accordingly, the Federal Constitutional Court has underlined that the security of the state, 100

as a constituted power of peace and order, as well as the security of the population it is bound to protect – while respecting the dignity and the intrinsic value of the individual – rank equally with other constitutional values that are accorded high standing. In view of this, the Court recognised a duty of the state to protect the life, physical integrity and liberty of the individual, which means in particular that the state must ensure protection against unlawful interferences by others (cf. BVerfGE 115, 320 <346 and 347>; cf. also BVerfGE 49, 24 <56 and 57>; 90, 145 <195>; 115, 118 <152 and 153>).

In assessing appropriateness, it must also be taken into account that the challenged provisions, even though the resulting interferences indiscriminately affect a large number of persons, do not affect the entire population to the same extent. Rather, these are predominantly provisions aiming to enable security authorities to avert, in individual cases, serious dangers threatening constitutionally protected legal interests as well as to prevent serious crime. 101

In light of the dangers posed by international terrorism, the decision to collect certain data is also of particular significance for information sharing between domestic authorities as well as for rendering the cooperation with foreign security authorities as effective as possible. Effective information sharing, which serves the constitutionally mandated protection of the individual, is contingent on the transfer of intelligence gathered domestically [to foreign authorities] and in return relies on intelligence provided by foreign authorities. 102

IV.

With regard to investigatory and surveillance powers constituting deep intrusions into the private sphere, which is the case for most of the powers at issue here, the Federal Constitutional Court has recognised certain general requirements deriving from the principle of proportionality in the strict sense. These requirements address specific large-scale risks to fundamental rights that potentially arise from such powers, including, in particular, risks arising from electronic data processing (cf. BVerfGE 100, 313 <358 *et seq*.>; 115, 320 <341 *et seq*.>; 125, 260 <316 *et seq*.>; 133, 277 <335 *et seq*. paras. 138 *et seq*.>), as well as risks arising where a surveillance measure taken in a particular case results in individuals affected by the measure coming under scrutiny by the authorities involved (BVerfGE 107, 299 < 312 *et seq*.>, BVerfGE 110, 33 <52 *et seq*.>; 113, 348 <364 *et seq*.>; 129, 208 <236 *et seq*.>, BVerfGE 109, 279 <335 *et seq*.>, BVerfGE 112, 304 <315 *et seq*.>, BVerfGE 120, 274 <302 *et seq*.>). 103

1. To the extent that covert surveillance measures reach deep into the private sphere, as most of the measures at issue here do, such measures are only compatible with the Constitution if they serve to protect or defend sufficiently weighty legal interests where there are reliable factual indications, in the specific case, suggesting that these interests are violated or at risk of being violated. In this regard, it must generally be established, based on the objective circumstances as examined by a rea- 104

sonable observer, that the person targeted by a measure is involved in the (potential) violation of protected legal interests. A mere possibility, based primarily on the intuition-based assumption of the security authorities in charge, that further intelligence might be gained does not provide sufficient grounds for carrying out such measures (cf. BVerfGE 107, 299 <321 *et seq*.>; 110, 33 <56>; 113, 348 <377 and 378, 380 and 381>; 120, 274 <328>; 125, 260 <330>). The Constitution thus sets clear limits to the lowering of statutory thresholds applicable to crime prevention measures if the measures in question are carried out covertly and potentially reach deep into the private sphere; in contrast, with regard to measures involving less intrusive interferences with the private sphere, the Constitution affords broader leeway to the legislator in crime prevention matters.

105 With regard to the specific design of the different statutory powers, the substantive assessment of whether they satisfy the requirements of appropriateness and specificity hinges on the weight of the interference resulting from each measure. The deeper the reach of surveillance measures into one's private life and the more they frustrate legitimate expectations of confidentiality, the stricter the requirements that the measures must satisfy. Among the measures at issue, surveillance of private homes and remote searches of information technology systems result in particularly deep intrusions into the private sphere.

106 a) Covert surveillance measures must be limited to the protection or defence of sufficiently weighty legal interests.

107 With regard to the measures that serve law enforcement purposes, and are thus repressive, this assessment depends on the weight of the criminal acts targeted by the measures. The legislator has divided the grounds for carrying out the measures into different categories of crime – considerable, serious and particularly serious – and defined each category in greater detail. For instance, the surveillance of private homes requires the suspicion of a particularly serious crime (cf. BVerfGE 109, 279 <343 *et seq*.>), telecommunications surveillance or the use of telecommunications traffic data stemming from precautionary data retention requires the suspicion of a serious crime (cf. BVerfGE 125, 260 <328 and 329>; 129, 208 <243>), while the collection of telecommunications traffic data based on specific grounds or observation by means of a GPS tracker, for example, requires the suspicion of a considerable crime – for surveillance targeting traffic data, the law furthermore specifies criminal offences that typically qualify as 'considerable crime' in this context – (cf. BVerfGE 107, 299 <321 and 322>; 112, 304 <315 and 316>; with regard to the latter decision, cf. also ECtHR, *Uzun v. Germany*, Judgment of 2 September 2010, no. 35623/05, § 70, NJW 2011, p. 1333 <1336>, regarding Art. 8 ECHR).

108 With regard to measures that serve to avert dangers to public security, and are thus preventive, this assessment depends on the weight of the legal interests that the measures serve to protect (cf. BVerfGE 125, 260 <329>). Covert surveillance measures that reach deep into a person's private life are only permissible to protect par-

ticularly weighty legal interests. These include life, limb and liberty of the person as well as the existence or security of the Federation or a *Land* (cf. BVerfGE 120, 274 <328>; 125, 260 <330>). By contrast, the Federal Constitutional Court has held that the unconditional protection of material assets does not necessarily constitute a sufficiently weighty interest in this context. At the same time, the Court has held that it is generally compatible with the Constitution to allow access to data retained as a precautionary measure (cf. BVerfGE 125, 260 <330>) or the surveillance of private homes also on the grounds of a danger to the general public (*gemeine Gefahr*) (cf. BVerfGE 109, 279 <379>), or to allow remote searches of information technology systems on the grounds of a danger to assets that affect the foundations of human existence and thus serve public interests (cf. BVerfGE 120, 274 <328>). Based thereon, the legislator is, however, not prevented from laying down uniform grounds, in terms of the protected legal interests, as the statutory threshold for carrying out these surveillance measures.

b) For the purposes of public security measures to protect the aforementioned legal interests, the collection of data by means of covert surveillance, which gives rise to very intrusive interferences, is generally only proportionate if there is a sufficiently specific and foreseeable danger to these legal interests in the individual case and the person targeted by these measures appears, from the perspective of a reasonable observer examining the objective circumstances, to be involved therein (cf. BVerfGE 120, 274 <328 and 329>; 125, 260 <330 and 331>). 109

The prerequisites applicable to such measures also depend on the type and weight of the respective interference. For the surveillance of private homes, which constitutes a particularly deep intrusion into the private sphere, Art. 13(4) of the Basic Law requires the existence of an acute danger (*dringende Gefahr*). 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 130, 1 <32>). 110

Furthermore, the prerequisites for establishing a sufficiently specific and identifiable danger to the aforementioned legal interests must correspond to the burden imposed on the persons affected by the measure. In general security law, the legal concepts of specific danger (*konkrete Gefahr*), immediate danger (*unmittelbar bevorstehende Gefahr*) or present danger (*gegenwärtige Gefahr*) are recognised as grounds for public security measures against persons responsible for a danger (*polizeipflichtige Personen*) in relation to one of the protected interests at issue here; these concepts set sufficient standards in line with constitutional law. The term ‘specific danger’, as traditionally used in police law, requires a situation where 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 an interest protected under public security law if the situation were to unfold without intervention (cf. BVerfGE 115, 320 <364>; BVerwGE 116, 347 <351>). […] 111

At the same time, constitutional law does not *per se* prevent the legislator from recognising grounds for interferences that, depending on the type of task and measure in question, differ from the traditional concepts of security law focused on averting specific, immediate or present dangers. Rather, the legislator may subject state action that aims to prevent criminal acts from being committed in the first place to less stringent limits in certain domains by lowering the standard of foreseeability regarding the causal chain [in the respective danger situation]. Yet the statutory basis of the measure constituting an interference must in any case require the existence of a sufficiently identifiable danger (*hinreichend konkretisierte Gefahr*), in the sense that there be at least factual indications that a specific danger to the protected legal interests may emerge. Assumptions based on general experience alone are not sufficient for justifying an interference. Rather, specific facts must be established that, in the individual case, support the prognosis that a chain of events leading to a violation of one of the protected legal interests will occur and that the situation can be attributed [to the person against whom the measure is directed] (cf. BVerfGE 110, 33 <56 and 57, 61>; 113, 348 <377 and 378>). A sufficiently identifiable danger in this sense may already exist even where the causal chain leading to the damage is not yet 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. Firstly, 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; secondly, the facts must 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 (BVerfGE 120, 274 <328 f.>; 125, 260 <330 f.>). With regard to terrorism, it must be taken into account that terrorist acts are often planned far in advance and carried out by lone individuals who have no criminal record, and that it is often not foreseeable where and how they will be carried out. In this regard, surveillance measures may be authorised even in cases where it is neither possible to determine what type of incident might occur nor to determine the timeframe in which it might occur, provided that the individual conduct of a person establishes the specific probability that they will commit some form of terrorist act in the not so distant future. For example, this might be the case where a person enters the Federal Republic of Germany after having attended a terrorist training camp abroad. 112

By contrast, the weight of interference resulting from covert police surveillance is not sufficiently taken into account where statutory provisions authorise the measure on grounds so precautionary in nature that the existence of a specific danger to the protected legal interests need no longer be foreseeable at all, not even with regard to its basic characteristics. Given the severity of interference, shifting the statutory threshold for exercising the powers in question to a purely precautionary stage is incompatible with the Constitution if it means that such measures could be carried out on grounds of relatively vague indications of possible dangers. […] 113

c) Constitutional law gives rise to a tiered system of requirements governing the extent to which surveillance measures may be carried out in respect of a target person's contacts where the affected persons themselves are not subject to any special responsibility, neither in the form of responsibility for actions or circumstances causing a danger nor in the form of responsibility as suspect of a crime. 114

Measures involving searches of information technology systems or the surveillance of private homes may only directly target persons that are responsible for impending or acute dangers (cf. BVerfGE 109, 279 <351, 352>; 120, 274 <329, 334>). These measures constitute such deep intrusions into the private sphere that they may not be extended to other persons as surveillance targets. Yet it is not constitutionally objectionable for measures targeting the persons responsible to also cover third parties, as long as this is unavoidable (cf. BVerfGE 109, 279 <352 *et seq*.>). Thus, the surveillance of the home of a third party may be authorised 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 investigation, and the surveillance of the target person's own home would not in itself be sufficient to investigate the case (cf. BVerfGE 109, 279 <353, 355 and 356>). 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 information relevant to the investigation, 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 investigation. 115

The ordering of other covert surveillance measures directly targeting third parties is not *per se* impermissible. It is conceivable that surveillance measures may be directed against persons associated with the target person, for instance (selected) persons belonging to the target person's contacts or persons used as messengers. Such surveillance powers can be justified by the purpose of public security as an objective interest, and by the interest in establishing the truth in criminal investigations. Where these surveillance measures are extended to third parties, they are subject to strict proportionality requirements and may only be authorised if there is a special individual link between the affected person and the danger or crime being investigated. […] 116

2. In procedural terms, too, the principle of proportionality gives rise to certain general requirements. For the most part, the investigation and surveillance measures in question entail very intrusive interferences, and it is to be expected that they will be carried out covertly and also record highly private information; it is therefore imperative that measures be in principle subject to prior review by an independent authority, for example in the form of a judicial warrant (cf. in this regard 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(3) and (4) of the Basic Law (cf. in this respect BVerfGE 109, 279 <357 *et seq*.>); for other measures, it directly follows from the principle of proportion- 117

ality (cf. BVerfGE 120, 274 <331 *et seq*.>; 125, 260 <337 *et seq*.>).

The legislator must set out the requirement of independent prior review in specific and clear provisions combined with strict standards regarding the content and the reasons of the warrant issued by the court. […] 118

3. In addition to the aforementioned constitutional standards relating to the general prerequisites for exercising such powers, the respective fundamental rights in conjunction with Art. 1(1) of the Basic Law give rise to further requirements for the protection of the core of private life where surveillance measures entail particularly intrusive interferences. 119

a) The constitutional protection of the core of private life guarantees the individual a domain of highly personal life that is free from surveillance. This protection is rooted in the respective fundamental rights affected by surveillance measures in conjunction with Art. 1(1) of the Basic Law and ensures a human dignity core that is beyond the reach of the state and provides fundamental rights safeguards against such measures. Even exceptionally significant interests of the general public cannot justify an interference with this domain of private life that is absolutely protected (cf. BVerfGE 109, 279 <313>; established case-law). 120

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 (cf. BVerfGE 109, 279 <313>; 120, 274 <335>; established case-law). 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, which is especially the case in a private home. Persons enjoying this highest level of trust include, in particular, spouses or partners, siblings and direct relatives in ascending or descending line, especially if they live in the same household, and can also include defence lawyers, doctors, clerics and close personal friends (cf. BVerfGE 109, 279 <321 *et seq*.>). This group only partially overlaps with the group of persons entitled to refuse to give evidence. Such conversations do no lose their overall highly personal character merely because they concern both highly personal and everyday matters (cf. BVerfGE 109, 279 <330>; 113, 348 <391 and 392>). 121

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. The discussion and planning of criminal acts is not part of the core of private life, but belongs to the social domain (cf. BVerfGE 80, 367 <375>; 109, 279 <319 and 320, 328>; 113, 348 <391>). This does not mean that the core protection were subject to a general balancing against public security interests. A highly personal conversation is not excluded from the core of private life simply because it might provide insights that could be helpful for the investigation of criminal acts or the averting of dangers to public security. Notes or statements made in the course of a conversation that only reveal, for instance, inner impressions and feelings and do not contain any indica- 122

tions pointing to specific criminal acts do not simply become relevant to the public because they might reveal the reasons or motives for criminal conduct (cf. BVerfGE 109, 279 <319>). Furthermore, despite having some link to criminal conduct, situations in which individuals are in fact encouraged to admit wrongdoing or to prepare for the consequences thereof, such as confessions or confidential conversations with a psychotherapist or defence lawyer, are part of the highly personal domain, which is completely beyond the reach of the state (cf. BVerfGE 109, 279 <322>). However, a sufficient link to the social domain does exist where conversations – even conversations with confidants – directly refer to specific criminal acts (cf. BVerfGE 109, 279 <319>).

b) Any 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 (cf. BVerfGE 109, 279 <318 and 319>; 113, 348 <390 and 391>; 120, 274 <335 *et seq*.>). Where the powers in question do not entail a risk of core violations, it is not necessary to enact such provisions. Yet when exercising those powers, too, limits directly arising from the Constitution regarding access to highly personal information must be respected in the individual case. 123

c) The protection of the core of private life is absolute and must not be made conditional upon a balancing against security interests under the principle of proportionality (cf. BVerfGE 109, 279 <314>; 120, 274 <339>; established case-law). Yet this does not mean that every instance in which highly personal information is collected amounts to a violation of the Constitution or of human dignity. Given that uncertainties are inherent in measures and prognoses carried out by security authorities in the context of their duties, an unintended intrusion upon the core of private life in the course of a surveillance measure cannot always be prevented from the outset (cf. BVerfGE 120, 274 <337 and 338>). However, the Constitution does require that surveillance powers be designed in such a way that the core of private life be respected as an absolute limit, which cannot be freely circumvented on a case-by-case basis. 124

aa) Thus, it is absolutely impermissible for the state to make the core of private life a target of investigations and to use information from the core in any way, including as the basis for further investigations. Targeted measures reaching into the highly private sphere – which does not include the discussion of criminal acts (see C IV 3 a above) – are ruled out from the outset, even if such measures could produce information that is helpful for the investigation. The protection of the core may not be subject to a balancing of interests in the individual case. 125

bb) Furthermore, it also follows that the protection of the core must be taken into account on two levels when carrying out surveillance measures. Firstly, at the stage of data collection, safeguards must be put in place to prevent the unintended collection of information relating to the core where possible. Secondly, at the stage of subsequent data analysis and use, the consequences of an intrusion upon the core of 126

private life that could not be prevented despite such safeguards must be strictly minimised (cf. BVerfGE 120, 274 <337 *et seq*.>; 129, 208 <245 and 246>).

d) In this context, the legislator may design the protection of the core of private life differently for different surveillance measures, depending on the type of power and its proximity to the absolutely protected domain of private life (cf. BVerfGE 120, 274 <337>; 129, 208 <245>). In doing so, it must, however, provide for safeguards at both stages. 127

At the data collection stage, with regard to measures with a high risk of core violations, a preliminary assessment must ensure that situations or conversations relating to the core are excluded in advance to the extent that this is feasible with reasonable effort (cf. BVerfGE 109, 279 <318, 320, 324>; 113, 348 <391 and 392>; 120, 274 <338>). With regard to conversations with persons enjoying the highest level of personal trust, circumstances that typically indicate a confidential setting may warrant the presumption that the communication is part of the core and must not be subject to surveillance (cf. BVerfGE 109, 279 <321 *et seq*.>; 129, 208 <247>). In the design of the statutory framework, the legislator may allow for a rebuttal of this presumption, in particular on the grounds of indications, in the individual case, that criminal acts will be discussed. By contrast, the presumption that a conversation is highly confidential cannot be rebutted solely on the grounds that, apart from highly personal matters, everyday matters will be discussed as well (cf. BVerfGE 109, 279 <330>). In any case, the measure must be discontinued when it becomes apparent that the surveillance is intruding upon the core of private life (cf. BVerfGE 109, 279 <318, 324, 331>; 113, 348 <392>; 120, 274 <338>). 128

At the stage of data analysis and use, the legislator must provide for cases in which it was not possible to avoid collecting information relating to the core. In this regard, the legislator must generally require that the collected data be screened by an independent body that removes information relating to the core prior to use by the security authorities (cf. BVerfGE 109, 279 <331 *et seq*.>; 120, 274 <338 and 339>). However, the procedural safeguards that are necessary under constitutional law do not, in every type of case, require that further independent bodies other than the investigating state authorities be established (cf. BVerfGE 129, 208 <250>). The necessity of such a screening depends on the type, as well as, if applicable, the design of the power in question. The more reliable the safeguards for preventing the collection of information relating to the core at the stage of data collection, the more the requirement of a screening by an independent body becomes dispensable, and vice versa. This does not alter the fact that the legislator may enact the statutory bases necessary to provide the investigation authorities of the state with the means to take action at short notice in exceptional cases of danger requiring immediate action (*Gefahr im Verzug*). In any case, the legislator must provide for the immediate deletion of any highly personal data collected and for mechanisms preventing any use of such data. The deletion must be documented in a manner that makes subsequent review possible (cf. BVerfGE 109, 279 <318 and 319, 332 and 333>; 113, 348 <392>; 120, 274 129

<337, 339>).

4. The combined effect of the different surveillance measures gives rise to distinct constitutional limits. Surveillance taking place over an extended period of time and covering almost every movement and expression of [private] life of the person under surveillance, which could be used as the basis for creating a personality profile, is incompatible with human dignity (cf. BVerfGE 109, 279 <323>; 112, 304 <319>; 130, 1 <24>; established case-law). The use of modern investigation methods, especially methods that cannot be perceived by affected persons, requires coordination on the part of security authorities to ensure, with regard to the potential harm inherent in 'additive' interferences with fundamental rights, that the overall extent of surveillance remains limited (cf. BVerfGE 112, 304 <319 and 320>). This applies without prejudice to the limits on data sharing between authorities arising from the principle of purpose limitation (see D I below). 130

5. Based on proportionality considerations, distinct constitutional limits to covert surveillance measures may also arise with regard to certain groups of professionals or other persons whose activities are recognised as meriting special confidentiality protection under the Constitution. The legislator must ensure that the authorities respect these limits when ordering and carrying out surveillance measures. 131

[…] 132-133

6. Moreover, the principle of proportionality sets requirements regarding transparency, individual legal protection, and administrative oversight (BVerfGE 133, 277 <365 para. 204>; cf. also BVerfGE 65, 1 <44 *et seq*.>; 100, 313 <361, 364>; 109, 279 <363 and 364>; 125, 260 <334 *et seq*.>; established case-law […]). The requirements applicable in this respect are derived from the affected fundamental right in conjunction with Art. 19(4) of the Basic Law (cf. BVerfGE 125, 260 <335>; 133, 277 <366 para. 206>). 134

The transparency of data collection and processing serves to contribute to securing trust and legal certainty, and to ensure that data processing [by the state] remains subject to a democratic discourse (BVerfGE 133, 277 <366 para. 206>). […] 135

a) Another requirement for the proportionate design of the surveillance powers in question is a statutory notification requirement. Given that surveillance measures must be carried out covertly in order to achieve their purpose, the legislator must ensure that the affected persons are generally notified, at least *ex post*, of the surveillance measures to allow the possibility of seeking individual legal protection in accordance with Art. 19(4) of the Basic Law. The legislator may provide for exemptions by balancing the interest in being notified against the constitutionally protected legal interests of third parties. The exemptions must, however, be limited to what is absolutely necessary (BVerfGE 125, 260 <336>). […] If there are compelling reasons preventing *ex post* notification, this must be confirmed by a judge and reviewed at regular intervals (BVerfGE 125, 260 <336 and 337>). 136

b) Given that the affected persons cannot assess with certainty whether and on what scale surveillance measures are carried out against them, the legislator must provide for rights to information [on the part of affected persons] that complement the state's powers to carry out information-related interferences. Restrictions of these rights are only permissible if they serve conflicting interests that outweigh the interest of affected persons in obtaining information. […] 137

c) In light of Art. 19(4) of the Basic Law, a proportionate design of surveillance measures further requires that following notification, affected persons be afforded a reasonable (*zumutbar*) possibility to seek judicial review of the measure's lawfulness (in this respect cf. also Arts. 51 and 52 of the Proposal for a Directive of the European Parliament and of the Council 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, […]). 138

[…] 139

d) With regard to covert surveillance measures, the transparency of data collection and processing as well as individual legal protection can only be ensured to a very limited degree, which is why the guarantee of effective administrative oversight is all the more significant. With regard to surveillance measures that reach deep into the private sphere, the principle of proportionality therefore gives rise to stringent requirements regarding the effective design of the oversight regime both at statutory level and in administrative practice (cf. BVerfGE 133, 277 <369 para. 214>). 140

The guarantee of effective administrative oversight requires the existence of a body vested with effective powers, such as, under current law, the Federal Data Protection Officer (cf., foundationally, BVerfGE 65, 1 <46>). […] 141

e) […] 142-143

7. The general requirements deriving from the principle of proportionality also entail deletion requirements (cf. BVerfGE 65, 1 <46>; 133, 277 <366 para. 206>; established case-law). These serve to ensure that the use of personal data remains limited to the purposes justifying the data processing measures, and that data can no longer be used once these purposes have been achieved. The deletion of the data must be documented to ensure transparency and oversight. 144

V.

The challenged surveillance powers under public security law fail to satisfy, in various respects, the constitutional requirements set out above with regard to the statutory prerequisites for the respective interferences. 145

1. § 20g(1) to (3) of the Federal Criminal Police Office Act is only in part compatible with the Constitution. 146

a) § 20g(1) of the Federal Criminal Police Office Act permits surveillance outside of private homes using the special means of data collection defined in greater detail in § 20g(2) of the Federal Criminal Police Office Act. It thus authorises interferences with the right to informational self-determination (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law) on the part of the Federal Criminal Police Office. 147

[…] 148

b) With regard to the weight of interference, § 20g(1) and (2) of the Federal Criminal Police Office Act covers a wide spectrum, also encompassing intrusive interferences. 149

The provision permits surveillance outside of private homes using the means listed in § 20g(2) of the Federal Criminal Police Office Act. These include in particular surveillance for extended periods, covert image recordings, the covert monitoring of non-public communication, the installation of tracking devices or the use of police informants and undercover police investigators. 150

The weight of interference of these measures can vary greatly. It ranges from interferences of low and medium weight, such as the taking of individual photos or simple observation for a limited time, 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 to register and audio-visually record as many statements and movements [of the target person] as possible with the help of modern technology, they can reach deep into the private sphere and thus constitute interferences of particularly great weight. 151

Like the averting of violations of other weighty legal interests or the prosecution of considerable criminal acts, the public interest in the effective prevention of terrorism can justify such interferences (see C II 3 a above), provided that the powers in question are designed in a proportionate manner. This is not fully the case here. 152

c) […] 153-161

d) § 20g(1) no. 2 of the Federal Criminal Police Office Act […] does not satisfy the constitutional requirements. The statutory prerequisites for carrying out the interferences neither satisfy the principle of specificity nor the principle of proportionality in the strict sense. 162

aa) As an addition to § 20g(1) no. 1 of the Federal Criminal Police Office Act, which is limited to averting dangers to public security, § 20g(1) no. 2 of the Federal Criminal Police Office Act extends the grounds for interference. The legislator's intent in creating the latter provision was that the measures should set in at an earlier stage, serving the prevention of crime. 163

Based on the standards set out above, the Constitution neither prevents the legislator from limiting, in principle, the grounds for security measures to the averting of specific dangers – in line with the traditional understanding of this concept –, nor does it require the legislator to stick to these traditionally recognised grounds. However, 164

even measures aimed at preventing criminal acts require a prognosis that is based on facts, rather than merely on general experience, indicating a specific danger. In principle, it must at least be possible to determine the type of incident that might occur, and that it will occur within a foreseeable timeframe (cf. BVerfGE 110, 33 <56 and 57, 61>; 113, 348 <377 and 378>; 120, 274 <328 and 329>; 125, 260 <330>). In respect of terrorist acts, the legislator may also recognise alternative grounds for carrying out surveillance measures where the individual conduct of a person establishes the specific probability that they will commit terrorist acts in the not so distant future (see C IV 1 b above). The requirements to this effect must be set out in clear statutory provisions.

bb) § 20g(1) no. 2 of the Federal Criminal Police Office Act does not satisfy these constitutional standards. While the provision does require, as grounds for the measure, the possibility that terrorist offences will be committed, the prerequisites for establishing a prognosis to this effect are too lenient. The provision does not prevent the authorities from working with a prognosis based solely on general experience. […] The provision therefore does not set sufficiently specific criteria for the authorities and courts to work with and could give rise to disproportionately broad measures. 165

e) […] 166-169

f) The procedural requirements set out in § 20g(3) of the Federal Criminal Police Office Act do not satisfy the principle of proportionality in all respects. 170

aa) […] 171

bb) § 20g(3) of the Federal Criminal Police Office Act does not sufficiently give effect to the requirement of obtaining prior judicial authorisation (*Richtervorbehalt*) deriving from the principle of proportionality. 172

[…] 173-174

g) Moreover, § 20g of the Federal Criminal Police Office Act fails to satisfy constitutional requirements to the extent that it does not provide for any protection of the core of private life. 175

§ 20g of the Federal Criminal Police Office Act authorises surveillance measures of varying quality and proximity to the private sphere. By also permitting long-term image recordings and long-term interception and recording of non-public communication, the provision authorises surveillance measures that typically intrude deeply into the private sphere. It is true that all these measures concern surveillance taking place outside of private homes. Yet this does not alter the fact that there is a certain risk that these measures will likely 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 – that can be attributed to the core of private life […]. 176

At least some of the powers laid down in that provision thus have a close link to the core of private life, which requires that protection of this core be guaranteed by an 177

express statutory provision. The legislator must provide for clear safeguards protecting the core both at the stage of data collection and at the stage of data analysis and use (see C IV 3 c bb, d above). Given that such safeguards are lacking, § 20g(1) and (2) of the Federal Criminal Police Office Act is not compatible with the Constitution in that respect either.

2. § 20h of the Federal Criminal Police Office Act, too, does not fully satisfy constitutional requirements. 178

a) § 20h of the Federal Criminal Police Office Act permits acoustic and visual surveillance in private homes. It thus constitutes an interference with Art. 13(1) of the Basic Law. 179

By authorising the surveillance of private homes, the provision gives rise to interferences with fundamental rights that are particularly serious. 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 109, 279 <313 and 314>). This does not rule out the possibility of surveillance, as set out in Art. 13(3) and (4) of the Basic Law. It is possible to justify such measures for the purposes of averting dangers posed by international terrorism (see C II 3 a above). Yet this is subject to particularly strict requirements, which § 20h of the Federal Criminal Police Office Act does not satisfy in every respect. 180

b) […] 181-185

c) […] 186

aa) […] 187-188

bb) […] 189-190

cc) The provision is incompatible with Art. 13(1) and (4) of the Basic Law insofar as it authorises the surveillance of private homes directed at a target person's contacts or associates (§ 20h(1) no. 1 c of the Federal Criminal Police Office Act). To this extent, it is disproportionate. 191

The surveillance of private homes is a particularly serious interference that intrudes deeply into the private sphere. The effects of such a measure are inherently more severe than those of surveillance measures outside of private homes or telecommunications surveillance. Its weight of interference is paralleled only by interferences targeting information technology systems. Thus, this type of surveillance only meets the requirement of appropriateness if it is exclusively restricted from the outset to conversations of the target person responsible for the danger in question (cf. BVerfGE 109, 279 <355>). In light of the severity of interference, it is disproportionate and impermissible to directly target third parties with this type of surveillance measures (see C IV 1 c above). 192

This does not alter the fact that surveillance of the target person's private home may also affect third parties in cases where this is unavoidable (cf. § 20h(2) third sentence 193

of the Federal Criminal Police Office Act). It may even be permissible, as discussed above, to carry out surveillance of the private homes of third parties where this serves to monitor the target person.

d) The procedural design of the powers to conduct surveillance of private homes does not raise constitutional concerns. In particular, the provision contains a requirement that the measure be authorised by a judge. […] 194

[…] 195

e) However, the protection of the core of private life provided for in § 20h(5) of the Federal Criminal Police Office Act is not fully in line with constitutional law. It does not satisfy the requirements deriving from Art. 13(1) in conjunction with Art. 1(1) of the Basic Law. 196

aa) Since the surveillance of private homes reaches deep into the private sphere and intrudes upon one's personal refuge, which is of fundamental importance for safeguarding human dignity, the constitutional requirements for protecting the core of private life are particularly strict (BVerfGE 109, 279 <313 *et seq*., 318 *et seq*., 328 *et seq*.>). 197

(1) 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 an effective protection of the core of private life (cf. BVerfGE 109, 279 <320>). Accordingly, conversations taking place in private spaces with persons enjoying the highest level of personal trust (see C IV 3 a above) are presumed to belong to the core of private life and may not be the target of surveillance (cf. BVerfGE 109, 279 <321 *et seq*.>). Automatic long-term surveillance of spaces in which such conversations are to be expected is therefore impermissible (cf. BVerfGE 109, 279 <324>). 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 a link exists, it is not cancelled out even 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. The mere expectation, however, that a conversation will concern both highly confidential and everyday matters is by itself not sufficient (cf. BVerfGE 109, 279 <330>, see C IV 3 a, d above). 198

Thus, if a surveillance measure is likely to intrude upon the core of private life, the measure must not be carried out. Yet if there are no such indications that there will be an intrusion upon the highly personal domain – also taking into account the above rules of presumption –, 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 (cf. BVerfGE 109, 279 <320, 323 and 324>). If it is not clear whether a situation is highly confidential – for example due to 199

language barriers –, or if there are specific indications suggesting that, along with highly private thoughts, criminal acts will also be discussed, surveillance in the form of automatic recordings may be continued.

(2) Specific constitutional requirements also arise at the stage of data analysis and use. It must be ensured that the information obtained through the surveillance measure will be screened by an independent body. This screening serves both as a review of lawfulness as well as a filter mechanism to remove highly confidential data, so that – to the greatest extent possible – such data is not disclosed to the security authorities. The independent body must be provided with all data stemming from the surveillance of private homes (cf. BVerfGE 109, 279 <333 and 334> […]). 200

Moreover, a prohibition of data use and deletion requirements, together with obligations to document the data deletion, must be put in place for cases where, despite all safeguards, information relating to the core of private life is nonetheless collected (see C IV 3 c bb, d, 7 above). 201

bb) Measured against these standards, § 20h(5) of the Federal Criminal Police Office Act satisfies the constitutional requirements at the stage of data collection, but not at the stage of data use. 202

[…] 203-205

3. With regard to electronic profiling and searches pursuant to § 20j of the Federal Criminal Police Office Act, the statutory prerequisites for interference are constitutionally unobjectionable. 206

[…] 207

4. If interpreted in conformity with the Constitution, § 20k of the Federal Criminal Police Office Act [which governs remote searches of information technology systems] is constitutional with regard to the general prerequisites for interference set out therein. However, the provision lacks sufficient safeguards to protect the core of private life in line with constitutional requirements. 208

a) […] 209-210

b) If interpreted in conformity with the Constitution, the requirements of § 20k(1) and (2) of the Federal Criminal Police Office Act regarding access to information technology systems satisfy the constitutional requirements. 211

aa) Interferences with the right to protection of the confidentiality and integrity of information technology systems are subject to strict conditions (cf. BVerfGE 120, 274 <322 *et seq*., 326 *et seq*.>). Specifically, the measures must be based on factual indications that a specific impending danger (*drohende konkrete Gefahr*) to an exceptionally significant legal interest exists in the individual case. § 20k(1) of the Federal Criminal Police Office Act satisfies this requirement. […] 212

However, a restrictive interpretation in conformity with the Constitution is merited 213

with regard to § 20k(1) second sentence of the Federal Criminal Police Office Act. That provision opens up the possibility of carrying out measures at a precautionary stage, prior to a specific danger, if specific facts indicate an impending danger of a terrorist act in the individual case; this must be interpreted to the effect that such measures are only permitted if the facts allow a determination as to the type of incident that might occur, and that it will occur in a foreseeable timeframe; the facts must also indicate the involvement of specific persons whose identity is known at least to such an extent that the surveillance measures can be targeted at and for the most part limited to them (BVerfGE 120, 274 <329>). Sufficient grounds for carrying out the measures also exist if neither the type of incident nor the expected timeframe are foreseeable yet, but the individual conduct of the targeted person establishes the specific probability that they will commit terrorist acts in the not so distant future (see C IV 1 b above).

The wording of § 20k(1) second sentence of the Federal Criminal Police Office Act closely resembles the wording adopted by the Federal Constitutional Court in past decisions (cf. BVerfGE 120, 274 <329>), which is why it can be assumed that the legislator intended to use the Court's case-law as point of reference. Based thereon, it is possible to interpret the provision in conformity with the Constitution. 214

bb) […] 215

c) […] 216

d) The safeguards to protect the core of private life, however, do not satisfy the constitutional requirements in every respect. 217

aa) Given that covert access to information technology systems typically entails the risk of recording highly confidential data, and thus bears a particularly close connection to the core of private life, it requires express statutory safeguards for the protection of the core (cf. BVerfGE 120, 274 <335 *et seq*.>). These constitutional requirements are not in every respect identical to those applicable to the surveillance of private homes, as they shift the protection away from the collection stage to the subsequent stage of analysis and use (cf. BVerfGE 120, 274 <337>). The reason for this lies in the specific nature of access to information technology systems. In this context, [and in contrast to the surveillance of private homes], protective safeguards against violations of the core of private life are not primarily aimed at preventing the recording and storing of a fleeting, highly personal and confidential moment in a private space, but rather at preventing the retrieval of highly confidential information from within an existing comprehensive data pool of digital information that, taken as a whole, is typically not of the same private nature as behaviour or communication in one's home. In this case, surveillance does not take place in the form of a chronological sequence in different locations, but rather in the form of access through a spy software, which, as far as access as such is concerned, offers only two alternatives: full access or no access at all. 218

In light of this, the constitutional standards for the protection of the core of private life are somewhat relaxed at the stage of data collection. Nevertheless, even at that stage, it must be ensured that any collection of information attributed to the core is refrained from to the extent that this is possible from a technical and investigative perspective. Available technical means must be used to implement such protection; where it is possible, through technical means, to identify and isolate highly confidential information, access to this information is prohibited (cf. BVerfGE 120, 274 <338>). 219

If, however, data relating to the core cannot be filtered out before or at the time of data collection, access to the information technology system is 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 in place safeguards at the stage of analysis and use, and by minimising the effects of such access. In this respect, the screening by an independent body that removes information relating to the core before the Federal Criminal Police Office can obtain knowledge thereof and use it is of particular significance (cf. BVerfGE 120, 274 <338 and 339>). 220

bb) § 20k(7) of the Federal Criminal Police Office Act does not fully satisfy these requirements. 221

[…] 222-226

5. § 20l of the Federal Criminal Police Office Act is only in part compatible with the Constitution. 227

a) § 20l of the Federal Criminal Police Office Act governs telecommunications surveillance, providing a statutory basis for interferences with Art. 10(1) of the Basic Law. […] 228

Telecommunications surveillance entails serious interferences (cf. BVerfGE 113, 348 <382>; 129, 208 <240>). Nevertheless, for the purpose of averting dangers from international terrorism, such interferences can be justified (see C II 3 a above) provided that the respective grounds for carrying out the interferences are restricted in a proportionate manner. Yet § 20l of the Federal Criminal Police Office Act only in part ensures that such restrictions are put in place. 229

b) § 20l(1) nos. 1 to 4 of the Federal Criminal Police Office Act provides different grounds for carrying out interferences [in the form of telecommunications surveillance] vis-à-vis different target persons. Not all of these grounds satisfy the constitutional requirements. 230

The authorisation to carry out surveillance measures against persons responsible for a danger under police law pursuant to § 20l(1) no. 1 of the Federal Criminal Police Office Act, which serves to protect qualified legal interests and has the sole purpose of averting acute dangers, does not raise constitutional concerns. 231

However, the extension of telecommunications surveillance pursuant to § 20l(1) no. 232

2 of the Federal Criminal Police Office Act to persons who, based on specific facts, are believed to be involved in the preparation of terrorist crimes is not compatible with the Constitution given that the grounds laid down therein are not sufficiently restricted. The provision shifts interference powers to a purely precautionary stage of preventing crime, before an actual danger arises; with its vague and open phrasing, it violates the principle of specificity and is disproportionately broad. […]

[…] 233

c) […] 234

d) […] 235

e) The provisions on the protection of the core of private life pursuant to § 20l(6) of the Federal Criminal Police Office Act are for the most part compatible with the Constitution. 236

aa) Telecommunications surveillance constitutes a serious interference that has a particularly close connection to the core. Given that content-related surveillance measures intercept all kinds of telecommunications-based exchanges, they typically entail the risk of also collecting highly private communication that falls within the protected core of private life. In this respect, special statutory safeguards must be put in place (cf. BVerfGE 113, 348 <390 and 391>; 129, 208 <245>). 237

However, in terms of its overall nature, telecommunications surveillance is not to the same extent characterised by an intrusion into the private sphere as the surveillance of private homes or remote searches of information technology systems (cf. BVerfGE 113, 348 <391>). It covers any kind of communication in any situation, as long as it is transmitted by technical means. In fact, only a small part of the contents that could be accessed by this type of surveillance measure qualifies as highly confidential; however, the risk of intercepting highly confidential communication is not an inherent feature of this surveillance measure – unlike in the case of the surveillance of a person's private refuge in a home. In that respect, telecommunications surveillance also differs from remote searches of information technology systems. […] Its potentially close link to the core of private life mainly stems from the fact that it may also result in the interception of highly personal communication between close confidants (cf. BVerfGE 129, 208 <247>). 238

The legislator may reflect these differences by providing for less strict requirements regarding the protection of the core. However, in this case, too, it must be assessed at the collection stage whether it is likely that highly private conversations will be intercepted and, if this is the case, the surveillance of such conversations must be prohibited. Where such conversations cannot be identified in advance with sufficient probability, the surveillance measures may be carried out, including – subject to a proportionality assessment – in the form of automatic long-term surveillance ordered in the individual case (cf. BVerfGE 113, 348 <391 and 392>; 129, 208 <245>). 239

As for ensuring protection of the core at subsequent stages, the law must provide for prohibitions to use data [relating to the core] as evidence and for deletion requirements, including a requirement that deletion be documented; by contrast, requiring a screening by an independent body is not always necessary in these cases (cf. BVerfGE 129, 208 <249>). Regarding telecommunications surveillance, the legislator may in fact make such screening conditional upon whether and to what extent it is likely that the surveillance measures will also touch on highly private information. This may overlap with the safeguards put in place at the data collection stage. 240

In this regard, the legislator has considerable latitude. […] 241

bb) § 20l(6) of the Federal Criminal Police Office Act for the most part satisfies these requirements. 242

[…] 243-246

6. […] 247-252

VI.

Measured against the general constitutional standards applicable to all investigatory and surveillance measures, too, the challenged powers are not compatible with the Constitution in several respects (see C IV 4 to 7 above). They require further provisions to ensure respect for the principle of proportionality. 253

1. It is not objectionable, however, that the Act does not contain an express provision that specifies in more detail the prohibition of sweeping surveillance with a view to the combined effect of the different powers (see C IV 4 above). Deriving from the principle of proportionality, the prohibition of sweeping surveillance serves to uphold the constitutionally required protection of the inalienable core of personality that is rooted in human dignity; when exercising surveillance powers, security authorities must observe this prohibition of their own accord (cf. BVerfGE 109, 279 <323>; 112, 304 <319>; 130, 1 <24>; established case-law). In this respect, it is not necessary to put in place further statutory provisions. […] 254

2. However, the level of protection afforded professional groups and other persons whose activities and communication merit special confidentiality protection under constitutional law does not satisfy the constitutional requirements in all respects. 255

[…] 256-258

3. The provisions governing the guarantees of transparency, legal protection, and administrative oversight do not satisfy the constitutional requirements in all respects either. 259

a) […] 260-262

b) […] 263-265

c) The design of administrative oversight does not satisfy the constitutional requirements (see C IV 6 d above). While the Federal Data Protection Act provides for oversight by the Federal Data Protection Officer, a body vested with adequate powers in that respect (cf. BVerfGE 133, 277 <370 para. 215>), it does not lay down sufficient statutory requirements ensuring that audits are performed at regular intervals not exceeding approximately two years (cf. BVerfGE 133, 277 <370 and 371, para. 217>). 266

[…] 267

d) […] 268

4. The rules governing the deletion of obtained data in § 20v(6) of the Federal Criminal Police Office Act also do not satisfy the constitutional requirements in all respects. 269

[…] 270-274

D.

Insofar as the constitutional complaints are directed against the powers relating to further data uses and the sharing of data with domestic and foreign authorities, the complaints are well-founded in several respects. 275

I.

The constitutional requirements applicable to further use and sharing of data collected by the state are informed by the principles of purpose limitation and change in purpose (cf. BVerfGE 65, 1 <51, 62>; 100, 313 <360 and 361, 389 and 390>; 109, 279 <375 *et seq*.>; 110, 33 <73>; 120, 351 <368 and 369>; 125, 260 <333>; 130, 1 <33 and 34>; 133, 277 <372 *et seq*. paras. 225 and 226>; established case-law). 276

Where the legislator permits the use of data beyond the specific grounds prompting the data collection and beyond the reasons justifying this data collection, it must create a separate statutory basis to that end (cf., e.g., BVerfGE 109, 279 <375 and 376>; 120, 351 <369>; 130, 1 <33>; established case-law). In this respect, the legislator may, firstly, provide for further use of the data within the purposes for which the data was collected. This approach is generally permissible under constitutional law provided that the legislator ensures that the further use of data adheres to the particular constitutional requirements set by the principle of purpose limitation (see 1 below). Secondly, the legislator may also allow a change in purpose. Given that this amounts to an authorisation for the use of data for new purposes, such a change in purpose is subject to specific constitutional requirements (see 2 below). 277

1. The legislator may allow that data is used beyond the specific investigation that prompted the data collection where this further use serves the same purpose as the original data collection. Such further use may be based on the reasons justifying the data collection in the first place and is thus not subject to the constitutional requirements applicable to a change in purpose. 278

a) The permissible scope of this type of further use depends on the statutory authorisation for the original data collection. The respective statutory basis determines the competent authority as well as the purposes and conditions of data collection, thereby defining the permissible scope of use. Accordingly, the use of the information thus obtained is not only limited to certain abstractly defined public tasks but actually subject to a purpose limitation determined by the collection purpose set out in the relevant statutory basis authorising the respective data collection. For that reason, further use of the data serving the purpose for which the data was originally collected is only permissible to the extent that the data is used by the same authority in relation to the same task and for the protection of the same legal interests as was the case with regard to the data collection. If the original authorisation to collect data is restricted to the purpose of protecting specified legal interests or preventing specified criminal offences, this purpose limits both the scope of immediate data use and the scope of further data uses, even if the data is still being handled by the same authority; other uses are only permissible if there is a separate statutory basis authorising such a change in purpose. 279

b) In principle, the purpose limitations that the same authority must observe, again, in each and every further use of the collected data do not include the relevant thresholds for exercising the data collection powers – this holds true for the threshold of sufficiently specific indications of danger, as traditionally required for public security measures, and the threshold of sufficient grounds for the suspicion of criminal conduct (*hinreichender Tatverdacht*), as required in the context of law enforcement. While the requirement of establishing sufficiently specific indications that an identifiable danger may emerge or a qualified suspicion of criminal conduct determines the permissible grounds of data collection, it does not determine the purposes for which the collected data may be used. 280

For that reason, it does not from the outset run counter to the principle that data be used only in accordance with the purpose for which it was originally collected if the authority in question is allowed to consider the data as mere evidentiary traces used, for the same task, as the basis for further investigations, without having to fulfil additional prerequisites. The authority may use the information thus obtained – either by itself or in combination with other available information – as a mere starting point for further investigations to protect the same legal interests in the context of the same task. In this regard, and within the limits set out above, the legal order recognises that the gathering of information – not least when aiming to understand terrorist structures – cannot be reduced to an exercise that merely stocks isolated individual data, with formal legal criteria determining which data items may be considered and which ones ought to be disregarded. […] 281

The principle of purpose limitation is satisfied if the authority that is authorised to collect data further uses this data while acting within the same remit for the protection of the same legal interests and the prosecution or prevention of the same criminal acts as specified in the statutory provision authorising the data collection. These re- 282

quirements are necessary, but generally also sufficient, to legitimise further use of the data in accordance with the principle of purpose limitation.

However, more stringent requirements arise from the principle of purpose limitation with regard to data obtained through the surveillance of private homes and remote searches of information technology systems: any further use of such data only satisfies the purpose limitation if it is also necessary to avert an acute danger (cf. BVerfGE 109, 279 <377, 379>) or an impending danger in the individual case (cf. BVerfGE 120, 274 <326, 328 and 329>), in keeping with the prerequisites applicable to the collection of such data. The extraordinary weight 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, including the permissible purposes, specified for the original data collection. Information thus obtained may not be used as evidentiary traces providing the basis for further investigations unless there is an acute danger or an impending danger in the individual case. 283

2. Moreover, the legislator may allow further data uses for purposes other than those for which the data was originally collected (change in purpose). In that case, however, the legislator must ensure that the weight of interference resulting from the data collection is also taken into consideration with regard to the new data uses (cf. BVerfGE 100, 313 <389 and 390>; 109, 279 <377>; 120, 351 <369>; 130, 1 <33 and 34>; 133, 277 <372 and 373 para. 225>). 284

a) The authorisation to use data for new purposes constitutes a separate interference with the fundamental right affected by the original data collection (cf. BVerfGE 100, 313 <360, 391>; 109, 279 <375>; 110, 33 <68 and 69>; 125, 260 <312 and 313, 333>; 133, 277 <372 para. 225>; cf. also ECtHR, *Weber and Saravia v. Germany*, Judgment of 29 June 2006, no. 54934/00, § 79, NJW 2007, p. 1433 <1434>, regarding Art. 8 ECHR). For that reason, changes in purpose must be measured against the fundamental rights that were affected by the data collection. This applies to any type of data use for purposes other than the purpose for which the data was originally collected, irrespective of whether the data is used as evidence or as a basis for further investigations (cf. BVerfGE 109, 279 <377>). 285

b) A change in purpose may only be authorised within the limits of the principle of proportionality. The weight attached to such a change in purpose in the balancing of interests is determined by the weight of interference of the data collection. Information obtained through measures constituting particularly intrusive interferences may only be used for particularly weighty purposes (cf. BVerfGE 100, 313 <394>; 109, 279 <377>; 133, 277 <372 and 373 para. 225>, with further references). 286

aa) In earlier decisions, the Federal Constitutional Court reviewed the proportionality of a change in purpose by determining whether the new use was “incompatible” with the original purpose of the data collection (cf. BVerfGE 65, 1, <62>; 100, 313 <360, 389>; 109, 279 <376 and 377>; 110, 33 <69>; 120, 351 <369>; 130, 1 <33>). This approach has since been developed further and now relies instead on the crite- 287

rion of a hypothetical recollection of data (*hypothetische Datenneuerhebung*). Where data obtained through intrusive surveillance and investigation measures is concerned, such as the data at issue in these proceedings, it is necessary to determine whether it would hypothetically be permissible, under constitutional law, to collect the relevant data again with comparably weighty means for the changed purpose (cf. BVerfGE 125, 260 <333>; 133, 277 <373 and 374 paras. 225 and 226>; substantively, this standard is not new as these considerations were already applied in BVerfGE 100, 313 <389 and 390> and referred to as a "hypothetical substitute interference" in BVerfGE 130, 1 <34>). The test 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 133, 277 <374 para. 226>). Thus, data sharing between authorities is not, in principle, ruled out simply because the authority receiving the data is – unlike the authority that permissibly collected the data and is now sharing it – not empowered to collect certain data itself as it has a different remit (cf. BVerfGE 100, 313 <390>). Furthermore, when creating provisions governing data sharing, legislative objectives such as simplification and practicability can justify the fact that the sharing of data is not subject to every single requirement applicable to the collection of data. However, the requirement that the new use must serve purposes of comparable weight must in any case be met.

bb) This means that a change in purpose requires that the new use of the data serve the protection of legal interests or the detection of criminal acts of such weight that it would be justified, under constitutional law, to collect the data again with comparably weighty means (cf. BVerfGE 100, 313 <389 and 390>; 109, 279 <377>; 110, 33 <73>; 120, 351 <369>; 130, 1 <34>). 288

Yet the requirements applicable to a change in purpose are not completely identical to the requirements applicable to the original data collection with regard to the degree of specificity required for establishing the existence of a danger or the suspicion of criminal conduct. Under the principle of proportionality, these requirements primarily establish the direct grounds for the data collection as such but not the grounds for further use of the collected data. An authorisation to use data for other purposes constitutes a separate interference that requires new justification. For that reason, such an authorisation requires its own, sufficiently specific grounds prompting the measure. Under constitutional law, it is thus necessary, but generally also sufficient, that the data – either by itself or in combination with other information available to the authority – creates a specific basis for further investigations. 289

Thus, with regard to the use of data by security authorities, 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 detect comparably serious criminal acts or to avert impending dangers that, at least in the medium term, threaten weighty legal interests that are comparable to the legal interests whose protection justified the collection of the relevant data. 290

The same, however, does not apply with regard to information obtained through the surveillance of private homes or through covert access to information technology systems. In view of the significant weight 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 danger (cf. BVerfGE 109, 279 <377, 379>) or a sufficiently identifiable danger in the specific case (see C IV 1 b above). 291

cc) These requirements, which must be met for a change in purpose to be permissible, specify and consolidate a long line of case-law developed by both Senates of the Federal Constitutional Court (cf. BVerfGE 65, 1 <45 and 46, 61 and 62>; 100, 313 <389 and 390>; 109, 279 <377>; 110, 33 <68 and 69, 73>; 120, 351 <369>; 125, 260 <333>; 130, 1 <33 and 34>; 133, 277 <372 and 373 para. 225>). This does not result in stricter standards but cautiously allows more leeway in the constitutional assessment given that the criterion of a hypothetical recollection of the data is not applied in a rigid manner (cf. already BVerfGE 133, 277 <374 para. 226>); it means that the traditional requirements regarding statutory thresholds for carrying out interferences, which determine the required temporal proximity of danger, are relaxed to some extent (cf. in particular BVerfGE 100, 313 <394>; 109, 279 <377>). If, on top of that, the requirement that the change in purpose serve comparably weighty legal interests were waived as well – as suggested in one of the dissenting opinions – the limits set by the principle of purpose limitation, as a core element of data protection under constitutional law (cf. BVerfGE 65, 1 <45 and 46, 61 and 62>), would practically be rendered meaningless in the domain of public security (or would only have rudimentary effects as these limits would no longer be applied except to data obtained through the surveillance of private homes or remote searches). This holds true all the more if the requirement of a specific basis for further investigations, too, were rejected as being overly strict. 292

II.

Based on these standards, § 20v(4) second sentence of the Federal Criminal Police Office Act, which governs how the Federal Criminal Police Office may use data it collected itself, does not satisfy the constitutional requirements. The provision is unconstitutional. 293

1. In principle, the use of data for the sole purpose of carrying out tasks serving the averting of dangers posed by international terrorism, as set out in § 20v(4) second sentence no. 1 of the Federal Criminal Police Office Act, is compatible with the Constitution; however, the provision lacks sufficient restrictions regarding the use of data obtained through the surveillance of private homes and remote searches. 294

[…] 295-302

2. § 20v(4) second sentence no. 2 of the Federal Criminal Police Office Act, which concerns the use of data for the purpose of protecting witnesses and other persons, 303

is also incompatible with the constitutional requirements. The provision merely makes a general reference to the tasks assigned to the Federal Criminal Police Office under § 5 and § 6 of the Federal Criminal Police Office Act but does not contain any kind of restriction. Therefore, the provision does not satisfy the requirement of specificity and, for that reason alone, fails to meet the standards set out above.

III.

§ 20v(5) of the Federal Criminal Police Office Act, which governs the sharing of data with other authorities, fails to satisfy the constitutional requirements in several respects. 304

1. § 20v(5) of the Federal Criminal Police Office Act provides various statutory grounds for the sharing of data, collected for the purpose of averting dangers posed by terrorism, with other authorities. With the various authorisations regarding data sharing, the legislator allows the use of that data for a changed purpose in the individual case and based on specific grounds. The legislator thus provides a basis for the use of data by other authorities, which – in accordance with the image of a double door – themselves must also be statutorily authorised to receive and use this data (cf. BVerfGE 130, 151 <184>). Thus, the provision provides for interferences with fundamental rights, which must, in each case, be measured against those fundamental rights that were affected by the collection of the data that is now being shared (cf. BVerfGE 100, 313 <360, 391>; 109, 279 <375>; 110, 33 <68 and 69>; 125, 260 <312 and 313, 333>; 133, 277 <372 para. 225; cf. also ECtHR, *Weber and Saravia v. Germany*, Judgment of 29 June 2006, no. 54934/00, § 79, NJW 2007, p. 1433 <1434>, regarding Art. 8 ECHR). 305

2. […] 306

3. […] The challenged powers are unconstitutional to the extent that the statutory prerequisites for data sharing fail to satisfy the standards developed above with regard to the test of a hypothetical recollection of data (see D I 2 b above). 307

a) […] 308-309

b) § 20v(5) first sentence no. 2 of the Federal Criminal Police Office Act governs the sharing of data for the purpose of averting dangers to public security. For the most part, it satisfies the constitutional requirements. However, the provision is disproportionate to the extent that it generally allows a transfer of data for the purpose of preventing certain criminal offences [without providing for sufficient restrictions]. 310

[…] 311-313

c) § 20v(5) first sentence no. 3 of the Federal Criminal Police Office Act, which governs the sharing of data for law enforcement purposes, is [also disproportionately broad and thus] not compatible with the Constitution. 314

[…] 315-318

d) § 20v(5) third sentence no. 1 of the Federal Criminal Police Office Act, which allows the sharing of data with the offices for the protection of the Constitution (*Verfassungsschutzbehörden*) and the Military Counter-Intelligence Service (*Militärischer Abschirmdienst*), is also incompatible with the constitutional requirements. 319

[…] 320

e) […] 321

4. Finally, with regard to all these data sharing powers, a general statutory framework is lacking that ensures sufficient administrative oversight. […] 322

IV.

In part, § 14(1) first sentence nos. 1 and 3, second sentence of the Federal Criminal Police Office Act, which governs the sharing of data with foreign authorities – to the extent that § 14a of the Federal Criminal Police Office Act is not applicable, which governs data sharing with EU Member States and which is not challenged in the present proceedings –, also does not satisfy the constitutional requirements. 323

1. Like the sharing of personal data with domestic authorities, the sharing of data with foreign authorities constitutes a change in purpose. In accordance with general standards, this change in purpose must be measured against the relevant fundamental rights affected by the original data collection (see D I 2 a above). At the same time, with a view to ensuring respect for foreign legal orders and values, certain constitutional standards that are specific to the sharing of data with other states apply. 324

a) After data has been shared with other states, the guarantees of the Basic Law can no longer be applied directly and the standards prevailing in the respective receiving state apply instead. Yet this does not generally prevent data sharing with other states. With its Preamble, together with Art. 1(2), Art. 9(2), Art. 16(2), Arts. 23 to 26 and Art. 59(2), the Basic Law binds the Federal Republic of Germany to the international community and programmatically commits German state authority to international cooperation (cf. BVerfGE 63, 343 <370>; 111, 307 <318 and 319>; 112, 1 <25, 27>). This includes interaction with other states even if their legal order and values do not fully conform to the German domestic conception (cf. BVerfGE 31, 58 <75 *et seq.*>; 63, 343 <366>; 91, 335 <340, 343 *et seq.*>; 108, 238 <247 and 248). Such data sharing also aims to maintain both intergovernmental relations in the mutual interest of the participating states and the Federal Government's capacity to act in the context of foreign policy (cf. BVerfGE 108, 129 <137>). 325

However, when deciding on the sharing of personal data with other states, German state authority essentially remains bound by the fundamental rights (Art. 1(3) of the Basic Law); yet the foreign state authority is only bound by its own legal obligations. 326

Therefore, fundamental rights set limits to data sharing, which serve to uphold data protection guarantees. The limits set by the Basic Law for the domestic collection and processing of data must not be undermined, in terms of their substance, by data shar- 327

ing between security authorities. The legislator must thus ensure that this fundamental rights protection is not eroded, neither by the sharing of data collected by German authorities with other states and international organisations nor by the receipt and use of data from foreign authorities that was obtained in violation of human rights.

Moreover, limits to data sharing arise with regard to the use of the data by the receiving state if there are concerns about human rights violations. Sharing data with other states is ruled out if there is reason to fear that its use could lead to violations of fundamental principles of the rule of law (cf. BVerfGE 108, 129 <136 and 137>). Under no circumstances may the state be complicit in violations of human dignity (cf. BVerfGE 140, 317 <para. 62>, with further references). 328

b) Accordingly, the sharing of data with other states must be restricted to sufficiently weighty purposes for which the data may be shared and used (see aa below); moreover, it must be ascertained that the data will be handled in accordance with the rule of law in the receiving state (see bb below). In addition, effective domestic oversight must extend to such data sharing (see cc below). Adherence to these requirements must be ensured through clear foundations in German law (see dd below). 329

aa) The requirements relating to the purpose of the sharing and use of the data [in the receiving state] derive from the constitutional criteria applicable to a change in purpose under German law (see D I 2 above). Data sharing requires that it were permissible to collect the shared data again, with comparably weighty means, for the purpose for which it is shared (criterion of a hypothetical recollection of data). Thus, data sharing must serve to detect comparably weighty criminal acts or to protect comparably weighty legal interests, depending on what was required for the original data collection. At the same time, data sharing does, in principle, not require sufficient indications of danger or grounds for the suspicion of criminal conduct; it is sufficient that the shared information, or the request by the receiving state, show that there is, in the individual case, a specific basis for further investigations for the purpose of detecting relevant criminal acts or averting impending dangers to relevant legal interests that may emerge at least in the medium term. However, stricter requirements apply to the sharing of data obtained through the surveillance of private homes and remote searches of information technology systems; in these cases, the interference thresholds applicable to the data collection must be fully met (see D I 2 b bb above; cf. also BVerfGE 109, 279 <377, 379>; 120, 274 <329 *et seq*.>). 330

It is therefore necessary, in particular when another state requests that data be shared, to assess the prospective use of data by the receiving state. This assessment 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 faces 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 331

identical manner, in the foreign legal order does not preclude data sharing with that state from the outset. When sharing the data, the receiving authorities must be informed in a clear and express manner of limitations restricting use of the shared data.

bb) Furthermore, the sharing of personal data with other states presupposes that the data be handled in accordance with human rights and data protection standards in the receiving state (see 1 below), which must be ascertained by the German state (see 2 below). 332

(1) The sharing of data with other states requires sufficient guarantees that the data will be handled in accordance with the rule of law in the receiving state. 333

(a) In terms of data protection standards, it is, however, 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. […] 334

However, the sharing of personal data with other states is only permissible if the handling of the shared data in these states does not undermine the protection of personal data guaranteed by human rights. […] 335

(b) 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) of the Basic Law). Overall, the legislator must ensure that the sharing of data collected by German authorities with other states 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) of the Basic Law). 336

(2) Ascertaining the necessary level of protection in the receiving state does not always require a comprehensive assessment in each individual case or binding assurances under international law. Instead, the legislator may allow this ascertainment to be based on a generalising assessment made by the Federal Criminal Police Office of the legal and factual situation in the receiving state. Such an assessment may be relied on unless there are facts to the contrary refuting the generalised assumptions in a particular case (cf. BVerfGE 140, 317 <para. 69>, with further references). 337

Where such generalised assessments of the situation in the receiving state are not tenable, it is necessary to conduct a fact-based assessment in the individual case; such an assessment must verify that adherence to essential requirements for the handling of data is sufficiently guaranteed (see D IV 1 b bb (1) above). […] 338

[…] 339

cc) In any case, the requirements of effective administrative oversight, including the proper documentation of data sharing activities as well as corresponding reporting 340

obligations, continue to apply in Germany (see C IV 6 d, e above).

dd) The standards set out above must be laid down in statutory provisions that satisfy the principles of specificity and legal clarity. This also applies to the design of statutory bases authorising, where permissible, a sharing of data for the purpose of obtaining information by cross-checking this data against data collected by authorities in other states and for receiving additional information on the relevant matter in return; these statutory bases, too, must be designed in line with the principle of legal clarity. 341

2. The prerequisites governing data sharing laid down in § 14(1) first sentence nos. 1 and 3 and second sentence of the Federal Criminal Police Office Act do not satisfy these requirements. 342

[…] 343-354

E.

I.

[…] 355-358

II.

In parts, the decision was not unanimous. […] 359

[…] 360

Kirchhof Gaier Eichberger

Schluckebier Masing Paulus

Baer Britz

Dissenting Opinion of Justice Eichberger

I cannot concur with this judgment, as I disagree in several respects with the conclusions regarding the challenged provisions, and with parts of the reasoning. 1

I.

The judgment summarises, consolidates and, in part, further develops the constitutional standards recognised in the Court's case-law regarding the collection of data by means of very intrusive investigation measures, and the sharing of such data, in the domain of counter-terrorism at issue here. I largely agree with the general standards laid down in the majority decision with regard to the different constitutional requirements governing the grounds for such investigation and surveillance measures and with regard to the requirements governing further use of information thus obtained. However, in several respects the Senate majority sets excessive requirements for such data collection and further use of the data. This is the case, in particular, for the obligations the Senate majority imposes on the legislator regarding the design of the statutory framework. As regards the decision on fundamental constitutional values, on the basis of which the Senate majority determines the permissibility of interferences with fundamental freedoms in view of the state's duty to ensure security, and on the basis of which it lays down specific constitutional requirements, the judgment does indeed draw on lines of case-law developed by the Court over the past twelve years. However, in my view, the degree of detail and rigidity of the requirements imposed on the legislator cannot be derived from the Constitution (cf. BVerfGE 125, 380, my dissenting opinion to BVerfGE 125, 260) 2

The standards set out by the Senate majority almost exclusively rely on an assessment of proportionality in the strict sense, that is a balancing of the burdens imposed on persons affected by very intrusive measures interfering with fundamental rights, on the one hand, and the state's duties of protection with regard to averting terrorist dangers, on the other. Yet the Senate does not sufficiently take into account the prerogative of assessment afforded the legislator when appraising the factual basis of dangers and making a prognosis on how such dangers may develop. Moreover, it is primarily for the legislator to weigh the legislative aims pursued. It is true that the Federal Constitutional Court may conduct, as part of the proportionality assessment in the strict sense, a thorough review of the legislator's weighing; however, the Court must not lose sight of its judicial mandate with respect to the legislator's prerogative of assessment and margin of appreciation in weighing the legitimate aim pursued. 3

With these considerations in mind, my starting point for the required balancing differs from the Senate majority's. This also leads me to different conclusions, in part with regard to the applicable general standards and especially with regard to the specific measures at issue. It is true that even the mere latent risk of covert surveillance and investigation measures exposes fundamental rights holders to burdens associated with the most severe interferences, and directly affects fundamental rights holders 4

where such measures are actually carried out against them. However, in weighing the potential risk posed by covert surveillance and investigation measures, it must be kept in mind that, for the most part, the challenged provisions do not authorise a general collection of data indiscriminately affecting a large number of persons. If, in a specific case, investigation measures affect persons that have not themselves provided grounds for the investigation or have only marginally contributed to such grounds, they may nevertheless be asked to endure the measure as a special sacrifice, as part of their duty as citizens, that serves to maintain public security. […]

[…] Not all of the requirements imposed on the legislator with regard to provisions governing procedure, transparency and oversight are actually prescribed, in exactly this form, by the Constitution – even if many of these requirements may be sensible and fitting. In my opinion, a significantly higher degree of judicial restraint would have been appropriate in the present case. Instead, though commendable in its attempt to consolidate existing case-law in a general introduction of sorts, the present judgment generalises previous findings in a manner that ultimately results in a problematic affirmation of excessive constitutional requirements in the domain at issue here […]. Clear statutory provisions are indispensable when it comes to very intrusive surveillance measures. At the same time, the statutory framework should be designed with a significantly higher degree of restraint, in terms of the level of detail, assuming that the security authorities can generally be trusted to take proportionate and lawful action in the individual case unless there are indications to the contrary. […] 5

II.

Even though, to the extent set out above, my approach differs from the approach taken by the Senate majority, I agree for the most part with the general standards laid down in the decision with regard to data collection and sharing, including the sharing of data with foreign authorities. I also concur, in large parts, with the conclusions derived from these standards with regard to the challenged provisions. These conclusions are convincing and well-reasoned. The resulting requirements for stringent legislation and obstacles to law enforcement must be tolerated in order to protect the fundamental freedoms concerned. Yet I consider the judgment's approach, though based on past decisions, to be excessive and not prescribed by constitutional law, both with regard to some of the observations made on general constitutional standards and with regard to the conclusions relating to the unconstitutionality of individual challenged provisions. In particular, this concerns the following aspects: 6

1. It is generally imperative that the Court practise more restraint when it comes to setting very detailed requirements for the legislator regarding the design of supplementary procedural and other safeguards; in any case, I think the judgment goes too far in deriving from the principle of proportionality the requirements that persons affected by very intrusive surveillance measures be afforded effective sanctioning mechanisms in addition to the right to seek a judicial review of lawfulness (see judgment C IV 6 c); that the oversight of data collection and use be carried out in regular 7

intervals not exceeding approximately two years (see judgment C IV 6 d); and that reporting obligations vis-à-vis Parliament and the public to ensure transparency and oversight be provided for since the data is collected covertly […]. It would have been sufficient to simply specify the level of protection that must be ensured by the legislator – anything beyond that constitutes unjustified overreach.

2. As for the different challenged investigation and surveillance measures, I believe the constitutional shortcomings to be much narrower in scope than what was found by the Senate majority. 8

a) The Senate majority considers various statutory authorisations to carry out certain investigation and data collection measures for the purposes of crime prevention to lack specificity and to be disproportionate (see judgment C V 1 d bb, 5 b, […]); in this regard, the Senate needlessly foregoes the possibility of interpreting the relevant provisions in conformity with the Constitution. […] 9

b) […] 10

c) Furthermore, I cannot concur with the Senate majority's view that § 20g of the Federal Criminal Police Office Act is unconstitutional for not sufficiently ensuring protection of the core of private life (see judgment C V 1 g). 11

Nevertheless, I do agree with the judgment's basic premise that it is incumbent upon the legislator to provide for safeguards and oversight where statutory provisions authorise surveillance and investigation measures that typically intrude upon the core of private life. This requires the legislator to provide for the various prerequisites set out in the judgment that aim to prevent the collection of data relating to the core in the first place; where the collection of such data cannot be fully prevented, the legislator must provide for screening and filtering at the stage of data analysis and processing, which must not be carried out by the security authority itself (see judgment C IV 3 d). […] 12

However, from my point of view, § 20g of the Federal Criminal Police Office Act does not authorise surveillance measures that typically lead to the collection of data relating to the core of private life […]. Measures taken pursuant to § 20g(2) of the Federal Criminal Police Office Act are generally carried out in public spaces, which contradicts the assumption that the information thus obtained typically includes data relating to the core. […] 13

3. If the further use of data obtained through surveillance measures entails a change in purpose, this amounts to a separate interference with the fundamental right affected by the original data collection. This is in line with established case-law, which I agree with. Yet some of the conditions laid out by the Senate majority regarding the permissibility of a change in purpose set the hurdles too high. In this respect, it is not adequately taken into account that the use for other purposes concerns data that has already been lawfully collected. 14

a) […] 15

b) […] As is the case with other surveillance measures entailing very intrusive interferences, in the context of the surveillance of private homes, too, the real and severe intrusion into the private sphere takes place when the authorities carry out the actual surveillance measure in the protected domain. While any further use, including for changed purposes, does indeed perpetuate this interference, it does not reach the level of severity of the initial interference, not even where the data is obtained through the surveillance of private homes (or remote searches of information technology systems for that matter). The further use, including a change in purpose, of information obtained through surveillance measures should only be measured against the general rules applicable in this regard. The Senate majority has missed the opportunity to correct its case-law accordingly. 16

Justice Eichberger

Eichberger

Dissenting Opinion of Justice Schluckebier

To the extent that the judgment objects to the challenged provisions under constitutional law, I agree neither with its outcome nor with its reasoning. 1

The Court's basic premise is correct in that it is incumbent upon the legislator to strike an appropriate balance between the interferences with fundamental rights that might arise, in the individual case, from the statutory provisions in question, and the state's duty to protect the fundamental rights of individuals and legal interests of the public in the context of preventing terrorist acts. However, based on that premise, the Senate majority conducts a proportionality assessment that I believe to be misguided, from a constitutional perspective, in several respects, and sets out excessive specificity requirements in relation to individual provisions. Moreover, the views laid down by the Senate majority have a serious impact on police laws of the *Länder,* yet these implications were not sufficiently addressed in the proceedings. Thus, the judgment restricts both the federal legislator's political latitude and, indirectly, the latitude of legislators of the *Länder* beyond what would have been appropriate. By laying down numerous requirements relating to technical legislative details, the Senate puts its own notion of how the statutory framework should be designed before that of the democratically legitimated legislator, even though it is the legislator that is held politically accountable for the legislative concept and that can adjust the law slightly where necessary; in my opinion, this goes too far. 2

Contrary to what the Senate majority assumed, some of the challenged provisions could in fact have been interpreted in conformity with the Constitution […] 3

[…] 4

I.

Before going into detail, it should be noted that the legislator, in designing the statutory framework aiming to effectively avert terrorist dangers and prevent crime, has essentially found an appropriate and tenable balance in the complex conflict between the fundamental rights of persons affected by the police measures, and the underlying statutory bases, on the one hand, and the legislator's duty to protect the fundamental rights of individuals and the constitutionally protected interests of the public on the other hand. The legislator thus gives effect to the principle that, in a state under the rule of law, individuals must be able to rely on effective protection *by* the state and on the protection of their freedoms *against* the state (see my dissenting opinion in BVerfGE 125, 364 <369>; regarding the state's duty to protect against terrorism and other threats see BVerfGE 120, 274 <319>). It is true that, in the individual case, the measures in question might also affect holders of fundamental rights who are not themselves suspected of terrorism or, as it later turns out, were wrongfully suspected at the time; yet they can be asked to endure the burdens arising from such measures as a special sacrifice demanded of them as members of the community. 5

After laying out general observations regarding the significance and weight attached to the aims pursued by the legislator, the reasoning of the judgment falls short when it comes to reviewing the individual provisions in question; here, the judgment neither properly assesses the proportionality in the strict sense nor the specificity of the challenged provisions. […] 6

As a result, I consider that the Senate majority's assessment of proportionality in the strict sense in relation to several of the challenged provisions is unconvincing and, in part, even fails to satisfy the element of appropriateness. This is confirmed by the fact that the challenged Act, and the statutory authorisations of interferences contained therein, have been in force for more than seven years now, yet, as the oral hearing revealed, the powers in question have only ever been applied in a few cases and, to date, there has been no evidence of shortcomings. […] 7

II.

I will now address some of the specific objections raised by the Senate majority: 8

1. The Senate finds the statutory prerequisites for carrying out the interferences, as set out in some of the challenged provisions, to be lacking on the grounds that the provisions did not subject the interferences to sufficiently stringent requirements and were therefore disproportionate and too unspecific […]. Yet it would have been possible, based on the considerations set out in the judgment, to interpret the prerequisites designed by the legislator in conformity with the Constitution. 9

2. The Senate majority held that the surveillance framework lacks an explicit statutory provision ensuring protection of the core of private life with regard to the special methods of data collection set out in § 20g(2) of the Federal Criminal Police Office Act, even where the surveillance measures are carried out outside the home and might differ, in terms of severity and proximity, in how closely they relate to the individual's private sphere. […] 10

I do not agree with this conclusion. In cases where technical surveillance measures take place outside the home, they generally do not affect a refuge typically considered private (BVerfGE 109, 279 <320 *et seq*.>). […] Thus, it was not necessary for the legislator to include an express provision protecting the core of private life. Rather, protection in this regard can be ensured when the law is applied in practice. 11

3. […] 12

[…] 13

4. Furthermore, I cannot support the reasoning by which the Senate majority requires the establishment of an "independent body" tasked with ensuring, in respect of data obtained through the surveillance of private homes and remote searches of information technology systems, protection of the core at the subsequent stages of data analysis and processing. […] 14

[…] 15

The rather complicated solution prescribed by the Court hampers the effectiveness of the envisaged measures, especially with regard to the surveillance of private homes, which means that ultimately these powers no longer constitute appropriate means for achieving the legislative aim pursued, namely effective protection against terrorism. […] 16

5. The Senate majority also criticises, based on proportionality considerations, the lack of procedural provisions supplementing the surveillance and investigatory powers to ensure transparency, legal protection and administrative oversight in all respects. Bearing in mind that the powers in question concern action, taken in the individual case, for the purposes of averting dangers posed by terrorism, I again consider the requirements set out in the judgment to be, at least in part, excessive. […] 17

[…] 18

III.

I also cannot concur with the Senate majority's finding that the challenged powers concerning further use of the data collected in the context of averting terrorist dangers and the sharing of such data with domestic and foreign authorities were unconstitutional. This applies in particular to the extent that the Senate majority permits the use of lawfully collected data in other contexts solely for the purposes of protecting the same or comparably weighty legal interests. This approach is only tenable in cases where information was obtained through particularly intrusive interferences, for instance, the surveillance of private homes or remote searches of information technology systems. However, in certain other cases where the information in question results from coincidental findings, it would be irresponsible, in my opinion, to leave weighty legal interests, whether of the individual or the public, unprotected due to rigorous doctrine. 19

1. The judgment makes the sharing and further use of the data dependent on whether, after the change in purpose, this data continues to serve the protection of legal interests or the detection of criminal acts of such weight that this could, by constitutional standards, justify collecting the data in question again with comparably weighty means (criterion of a hypothetical recollection of data). This approach may be tenable with regard to information obtained through highly intrusive and particularly serious interferences, which is the case, for example, when methods such as surveillance of private homes and remote searches were used to collect the data. However, with regard to other types of interferences, which result in so-called coincidental findings, this approach, in my opinion, would lead to hardly tolerable results since it requires the legal order, which is committed to the rule of law, to stand back and ignore impending dangers to other legal interests that are sufficiently weighty, allow crimes to happen and legal interests to be violated. In this scenario, the state fails to fulfil its duty of protection. 20

[…] 21-24

2. […] 25

3. […] 26-27

4. […] 28

As the real challenge lies in the application of the law in the individual case, the additional statutory provisions, as required by the Senate majority, will not provide a viable solution. Once again, the insertion of additional detailed provisions into the existing legislative framework, as is now required of the legislator, will inflate the legislative text further, rendering the already excessively long statute even less legible and comprehensible – which ultimately leads to the opposite of legal clarity. At the same time, it would not even benefit affected persons, given that it will hardly lead to any measurable strengthening of protection in practice. 29

Justice Schluckebier

Schluckebier

Bundesverfassungsgericht, Beschluss des Ersten Senats vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09

Zitiervorschlag BVerfG, Beschluss des Ersten Senats vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09 - Rn. (1 - 29), http://www.bverfg.de/e/rs20160420_1bvr096609en.html

ECLI ECLI:DE:BVerfG:2016:rs20160420.1bvr096609