Headnotes

to the Judgment of the First Senate of 2 March 2010

1BvR 256, 263, 586/08

1. **The precautionary retention of telecommunications traffic data by private service providers without specific grounds, for a period of six months, as provided for under Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 (OJ L 105 of 13 April 2006, p. 54; hereinafter: Directive 2006/24/EC), is not *per se* incompatible with Art. 10 of the Basic Law; there is thus no need to decide on the possible precedence of the directive over domestic law.**

2. **The principle of proportionality requires that the statutory framework governing such data retention be designed so as to adequately reflect the particular weight of the resulting fundamental rights interference. This requires sufficiently stringent and clear statutory provisions regarding data security, data use, transparency and legal protection.**

3. **Under Art. 73(1) no. 7 of the Basic Law, it is incumbent upon the federal legislator to enact provisions ensuring data security and to subject possible data use to a clear purpose limitation, as these elements are inseparable from the statutory provisions imposing obligations to retain data. By contrast, the legislative competence for enacting provisions governing requests for access to the retained data by the authorities, and for specifying the applicable transparency and legal protection regime, lies with the legislator that is competent to legislate on the respective underlying subject matter.**

4. **With regard to data security, the legislator must lay down particularly high standards in clear and binding provisions. These provisions must ensure that, in principle, the required level of data security is informed by the current state of expertise and incorporates, on an ongoing basis, new research and advances in this field. It must also be ensured that data security may not be freely weighed against general business considerations.**

5. **Requests for access to and the direct use of retained data are only proportionate if they serve to protect exceptionally significant legal interests. In the domain of law enforcement, this requires that specific facts give rise to the suspicion of serious criminal acts. In the domain of public security and the tasks of the intelligence services, requests for data access and use of the data may only be authorised if there are factual indications of a specific danger to life, limb or liberty of the person or to the existence or security of the Federation or a *Land*, or of a danger to the general public.**

6. **The mere indirect use of the data by telecommunications service providers to provide information to the authorities on the subscribers of Internet Protocol addresses is permissible for the purposes of law enforcement, public security and the tasks of the intelligence services, even where this is not subject to a narrowly-defined statutory catalogue of criminal offences or protected legal interests. For prosecuting administrative offences [as a law enforcement purpose], such information may only be provided to the authorities in cases of particular weight on grounds expressly set out in the law.**

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 256, 263, 586/08 -

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaints of

I.

1. Prof. Dr. G…, 2. Dr. G…, 3. Mr K…, 4. J… GmbH, represented by its managing director, 5. Mr U…, 6. Mr R…, 7. Mr Z…, 8. Dr. B…,

– authorised representative: …

against §§ 113a and 113b of the Telecommunications Act as amended by the Act Revising the Law on Telecommunications Surveillance and Other Covert Investigation Measures and Transposing Directive 2006/24/EC of 21 December 2007 (BGBl I, p. 3198)

- 1 BvR 256/08 -,

II.

1. Dr. Dr. h. c. H…, 2. Dr. S…, 3. Ms L…, 4. Mr B…, 5. Ms P…, 6. Mr K…, 7. Dr. L…, 8. Dr. W…, 9. Prof. Dr. S…, 10. Ms S…, 11. Mr F…, 12. Mr S…, 13. Mr V…, 14. Mr W…,

– authorised representative: …

against the Act Revising the Law on Telecommunications Surveillance and Other Covert Investigation Measures and Transposing Directive 2006/24/EC of 21 December 2007 (BGBl I, p. 3198)

- 1 BvR 263/08 -,

III.

1. Ms A…, 2. Ms B..., 3. Mr B..., 4. Ms B…, 5. Ms B..., 6. Mr B…, 7. Mr D..., 8. Dr. D..., 9. Dr. E..., 10. Mr F..., 11. Mr G..., 12. Ms G..., 13. Ms H..., 14. Ms H..., 15. Ms H..., 16. Mr H..., 17. Mr H..., 18. Mr W..., 19. Mr W..., 20. Mr T..., 21. Dr. T..., 22. Mr S..., 23. Dr. S..., 24. Ms S..., 25. Ms S..., 26. Ms S..., 27. Ms S..., 28. Ms P..., 29. Mr N..., 30. Mr N..., 31. Ms M..., 32. Mr M..., 33. Ms M..., 34. Ms L..., 35. Ms K..., 36. Mr K..., 37. Mr K..., 38. Ms K..., 39. Ms K..., 40. Dr. H..., 41. Ms H..., 42. Ms H..., 43. Ms H...,

– authorised representative: …

against the provisions on data retention in the Act Revising the Law on Telecommunications Surveillance and Other Covert Investigation Measures and Transposing Directive 2006/24/EC of 21 December 2007 (BGBl I, p. 3198)

- 1 BvR 586/08 -

the Federal Constitutional Court – First Senate –

with the participation of Justices

President Papier,

Hohmann-Dennhardt,

Bryde,

Gaier,

Eichberger,

Schluckebier,

Kirchhof,

Masing

held on the basis of the oral hearing of 15 December 2009:

JUDGMENT

1. **§§ 113a and 113b of the Telecommunications Act, as amended by Article 2 no. 6 of the Act Revising the Law on Telecommunications Surveillance and Other Covert Investigation Measures and Transposing Directive 2006/24/EC of 21 December 2007 (BGBl I, p. 3198), violate Article 10(1) of the Basic Law and are void.**

2. **§ 100g(1) first sentence of the Code of Criminal Procedure, as amended by Article 1 no. 11 of the Act Revising the Law on Telecommunications Surveillance and Other Covert Investigation Measures and Transposing Directive 2006/24/EC of 21 December 2007 (BGBl I, p. 3198), violates Article 10(1) of the Basic Law and is thus void to the extent that it permits the obtaining of traffic data retained pursuant to § 113a of the Telecommunications Act.**

3. **The telecommunications traffic data that was compiled and temporarily stored by providers of publicly available telecommunications services at the request of the authorities but not yet transferred to the respective requesting authority under § 113b first sentence, first half-sentence of the Telecommunications Act in accordance with the preliminary injunction issued on 11 March 2008 in the proceedings 1 BvR 256/08 (BGBl I, p. 659), repeated and extended by Order of 28 October 2008 (BGBl I, p. 2239), last repeated by Order of 15 October 2009 (BGBl I, p. 3704), must be deleted without undue delay. The data may not be transferred to the requesting authorities.**

4. **[…]**

REASONS:

A.

The constitutional complaints concern provisions of the Telecommunications Act and the Code of Criminal Procedure that govern the precautionary retention of telecommunications traffic data by the providers of publicly available telecommunications services for a period of six months, and the use of such data. 1

I.

The challenged provisions […] serve to transpose Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105 of 13 April 2006, p. 54; hereinafter: Directive 2006/24/EC). 2

1. All constitutional complaints directly challenge §§ 113a and 113b of the Telecommunications Act, which were inserted into the Telecommunications Act by Art. 2 no. 6 of the Telecommunications Surveillance Revision Act. Furthermore, the constitutional complaints in proceedings 1 BvR 263/08 and 1 BvR 586/08 directly challenge § 100g of the Code of Criminal Procedure, as amended by Art. 1 no. 11 of the Telecommunications Surveillance Revision Act, to the extent that it permits the authorities to obtain data retained pursuant to § 113a of the Telecommunications Act. 3

a) § 113a of the Telecommunications Act aims to ensure that for all publicly available telecommunications services, traffic data providing information on the lines used in telecommunications, and on the time and location of the communication, be retained for six months and kept available so that it can be used by the authorities in the exercise of their functions. […] 4

§ 113a(1) first sentence of the Telecommunications Act obliges providers of publicly available telecommunications services to retain, for a period of six months, the telecommunications traffic data listed in § 113a(2) to (5) regarding phone calls via landlines, the Internet and mobile phones, transmission of text messages, multi-media messages and similar messages, email communications and Internet access. […] Pursuant to § 113a(11) of the Telecommunications Act, the data must be deleted within one month after the retention period expires. Pursuant to § 113a(8) of the Telecommunications Act, neither the contents of communications nor data on accessed websites may be retained. […] 5

In addition to the data retention pursuant to § 113a of the Telecommunications Act, the providers of telecommunications services may continue to store and use telecommunications traffic data pursuant to § 96 of the Telecommunications Act if it is necessary for the purposes specified in that provision. […] 6

[…] 7-37

b) § 113b of the Telecommunications Act sets out the purposes for which the data retained pursuant to § 113a of the Telecommunications Act may be used. […] 38

aa) […] 39

[…] 40-42

bb) In principle, § 113b first sentence, second half-sentence of the Telecommunications Act rules out the use of data retained pursuant to § 113a of the Telecommunications Act for purposes other than those stated in § 113b first sentence, first half-sentence of the Telecommunications Act. However, it provides for the exception that retained data may also be used by service providers for the purposes of providing certain information to the authorities pursuant to § 113 of the Telecommunications Act. 43

§ 113(1) of the Telecommunications Act permits the authorities to request the transfer of so-called customer and subscriber data pursuant to §§ 95 and 111 of the Telecommunications Act, in particular telephone numbers, subscriber line identifications, and the names and addresses of subscribers. […] 44

[…] 45-46

Information pursuant to § 113(1) first sentence of the Telecommunications Act must be provided to the authorities upon request if it is necessary for prosecuting criminal or administrative offences, averting dangers to public security and order, or for the tasks of the intelligence services. 47

cc) […] 48-60

c) § 100g(1) first sentence of the Code of Criminal Procedure sets out to what extent telecommunications traffic data may be obtained for law enforcement purposes. According to this provision, law enforcement authorities may […] access traffic data stored by telecommunications companies on the basis of § 96 of the Telecommunications Act. Apart from this, § 100g of the Code of Criminal Procedure now also permits authorities to obtain data retained as a precautionary measure pursuant to § 113a of the Telecommunications Act. […] 61

[…] 62-79

2. […] 80-86

3. […] 87

4. […] 88

II.

1. The complainants in proceedings 1 BvR 256/08 challenge §§ 113a and 113b of the Telecommunications Act. They claim a violation of Art. 10(1), Art. 12(1), Art. 14(1), Art. 5(1) and Art. 3(1) of the Basic Law. […] 89

[…] 90-116

2. The complainants in proceedings 1 BvR 263/08 challenge §§ 113a and 113b of the Telecommunications Act as well as § 100g of the Code of Criminal Procedure to the extent that it concerns the obtaining of data retained pursuant to § 113a of the Telecommunications Act. They claim a violation of Art. 1(1), Art. 2(1) in conjunction with Art. 1(1), Art. 10(1) and Art. 19(2) of the Basic Law. 117

[…] 118-133

3. The complainants in proceedings 1 BvR 586/08 also challenge §§ 113a and 113b of the Telecommunications Act and § 100g of the Code of Criminal Procedure. They claim a violation of Art. 10(1) and Art. 2(1) in conjunction with Art. 1(1) of the Basic Law. 134

[…] 135-145

III.

Statements on the constitutional complaints were submitted by the Federal Government, the Federal Administrative Court, the Federal Court of Justice, the Federal Officer for Data Protection and Freedom of Information, and, on behalf of the *Länder*, the Berlin Officer for Data Protection and Freedom of Information. 146

1. […] 147-164

2. […] 165

3. […] 166

4. […] 167-170

5. […] 171

6. Statements on the Court's technical, factual and legal questions were submitted by Constanze Kurz, Prof. Dr. Felix Freiling, Prof. Dr. Andreas Pfitzmann, Prof. Dr. Alexander Roßnagel, Prof. Dr. Christoph Ruland, the Federal Officer for Data Protection and Freedom of Information, the Berlin Officer for Data Protection and Freedom of Information, the Federal Ministry of Justice with the participation of the Federal Ministry for Economic Affairs and Technology and the Minister of the Interior, the complainants in proceedings 1 BvR 256/08 and 1 BvR 263/08 as well as the Federal Association for Information Technology, Telecommunications and New Media (*Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.*, BITKOM), the eco Association of the German Internet Industry (*Verband der deutschen Internetwirtschaft e.V.*, eco) as well as the Association of Telecommunications and Value-Added Service Providers (*Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V.*, VATM). 172

7. […] 173

IV.

[…] 174

B.

The constitutional complaints are admissible. 175

[…] 176-182

C.

The constitutional complaints are for the most part well-founded. The challenged provisions violate the complainants' fundamental right under Art. 10(1) of the Basic Law. There is no reason to request a preliminary ruling from the Court of Justice of the European Union, since the possible precedence of Community law is not relevant in the present proceedings. The fundamental rights guarantees of the Basic Law do not preclude the transposal of Directive 2006/24/EC provided that the legislator revises the design of the statutory framework. 183

The constitutional complaint of complainant no. 4 in proceedings 1 BvR 256/08 is unfounded to the extent that it claims a violation of Art. 12(1) of the Basic Law. 184

I.

[…] 185-187

II.

The challenged provisions interfere with Art. 10(1) of the Basic Law. 188

1. Art. 10(1) of the Basic Law guarantees the privacy of telecommunications, which protects the non-physical transmission of information to individual recipients by way of telecommunications traffic (cf. BVerfGE 106, 28 <35 and 36>; 120, 274 <306 and 307>) against public authorities obtaining knowledge thereof (cf. BVerfGE 100, 313 <358>; 106, 28 <37>). This protection is not limited to the actual communication contents. It also extends to the confidentiality of the specific circumstances of a communication, which include in particular whether, when and how often telecommunications traffic occurred or was attempted between whom or between which devices (cf. BVerfGE 67, 157 <172>; 85, 386 <396>; 100, 313 <358>; 107, 299 <312 and 313>; 115, 166 <183>; 120, 274 <307>). 189

The protection under Art. 10(1) of the Basic Law applies not only to the initial access, whereby public authorities obtain knowledge of telecommunications activities and contents for the first time. This fundamental right also protects against information and data processing measures that follow after the state obtained knowledge of protected communications, and against any subsequent use of the information thus obtained (cf. BVerfGE 100, 313 <359>). Any instance where the state obtains knowledge of, stores or processes telecommunications data, any analysis of communication contents, and any other use by public authorities constitutes an interference with fundamental rights (cf. BVerfGE 85, 386 <398>; 100, 313 <366>; 110, 33 <52 and 53>). Hence, the collection and storage of telecommunications data, the cross-checking with other data, the analysis of the data, its selection for further use, or the transfer to third parties each constitute a separate interference with the privacy of telecommunications (cf. BVerfGE 100, 313 <366 and 367>). Consequently, the obligations imposed on telecommunications companies to collect telecommunications data, to retain it, and to transfer it to state authorities all constitute separate interferences with Art. 10(1) of the Basic Law (cf. BVerfGE 107, 299 <313>). 190

The right to informational self-determination following from Art. 2(1) in conjunction with Art. 1(1) of the Basic Law is not applicable in addition to Art. 10 of the Basic Law since, in the context of telecommunications, Art. 10 of the Basic Law contains a more specific guarantee that supersedes the aforementioned general guarantee and that gives rise to special requirements where data is obtained through interferences with the privacy of telecommunications. Yet the requirements that the Federal Constitutional Court derived from Art. 2(1) in conjunction with Art. 1(1) of the Basic Law can largely be applied accordingly to the more specific guarantee of Art. 10 of the Basic Law, too (cf. BVerfGE 100, 313 <358 and 359>). 191

2. a) The obligation to retain telecommunications traffic data imposed on service providers under § 113a(1) of the Telecommunications Act interferes with the privacy of telecommunications. Firstly, this holds true for the obligations to retain data imposed on service providers in § 113a(2) to (5) of the Telecommunications Act, and for the retention obligation that derives from § 113a(2) to (5) of the Telecommunications Act in conjunction with § 113a(6) and (7) of the Telecommunications Act. The data to be retained pursuant to these provisions provides information on whether, when, where and how often connections were established or attempted between which devices. In particular, this also extends to the retention of data concerning email services pursuant to § 113a(3) of the Telecommunications Act, whose confidentiality is equally protected by Art. 10(1) of the Basic Law (cf. BVerfGE 113, 348 <383>; 120, 274 <307>). While intercepting emails may be simple from a technical point of view, this does not alter the fact that such communication is regarded as confidential and merits protection. Retaining data relating to Internet access pursuant to § 113a(4) of the Telecommunications Act also interferes with Art. 10(1) of the Basic Law. It is true that Internet access enables not only communication between individuals, which is protected by the privacy of telecommunications, but also participation in mass communication. However, it is not possible to distinguish between individual and mass communication without determining the contents of the information transmitted in each case, which would actually run counter to the protection the fundamental right seeks to afford; therefore the retention of data relating to Internet access as such must already be regarded as an interference, even where this data does not include any information on accessed websites […]. 192

The finding that § 113a of the Telecommunications Act gives rise to interferences is not called into question by the fact that the data retention required by this provision is not carried out directly by the state but by private service providers. This is because the state merely uses these service providers as agents assisting in the exercise of state functions. § 113a of the Telecommunications Act obliges private telecommunications companies to retain data solely so that state authorities can fulfil their responsibilities pursuant to § 113b of the Telecommunications Act, for the purposes of law enforcement, public security and the tasks of the intelligence services. The impairment of fundamental rights resulting from data retention is directly ordered by the state, without affording the companies obliged to retain data any discretion; they are obliged to retain the data in a manner that enables them to comply with information requests by authorised public authorities pursuant to § 113a(9) of the Telecommunications Act without undue delay. Under these conditions, the retention of data must be qualified as a direct interference with Art. 10(1) of the Basic Law that is legally attributable to the legislator (cf. BVerfGE 107, 299 <313 and 314>). 193

b) The data transfers to the authorities set out in § 113b first sentence, first half-sentence of the Telecommunications Act also result in interferences with Art. 10(1) of the Basic Law. It is true that the statutory provision does not directly permit the use of data retained pursuant to § 113a of the Telecommunications Act; instead, reference 194

is made to other, separate legislation, which has yet to be enacted, based on which access to the data may then be requested by the authorities. The aforementioned provision does, however, already contain a basic determination of the purposes for which such data may ultimately be used. […] As the envisaged transfer of data derives from a statutory provision, it is directly based on an act of public authority bound by fundamental rights under Art. 1(3) of the Basic Law; the transfer requires an authorising state order in each individual case; and the recipients of the transfer are state authorities. In legal terms, it must therefore be qualified as a state interference.

c) § 113b first sentence, second half-sentence in conjunction with § 113(1) of the Telecommunications Act also gives rise to an interference with Art. 10(1) of the Basic Law. It provides that the authorities may request information from service providers on subscriber and customer data pursuant to §§ 95 and 111 of the Telecommunications Act, which they can only provide by using the data retained pursuant § 113a(4) of the Telecommunications Act. It is not relevant in this respect whether and to what extent providing information pursuant to § 113 of the Telecommunications Act generally constitutes an interference with Art. 10(1) of the Basic Law or whether, in principle, only the right to informational self-determination under Art. 2(1) in conjunction with Art. 1(1) of the Basic Law is applicable. In any case, an interference with the privacy of telecommunications under Art. 10(1) of the Basic Law arises at least where information is provided on the basis of § 113b first sentence, second half-sentence and § 113(1) of the Telecommunications Act. This is due to the fact that it concerns the use of data retained pursuant to § 113a of the Telecommunications Act, which means it was obtained through an interference with Art. 10(1) of the Basic Law. Where data was originally obtained through an interference with Art. 10(1) of the Basic Law, any subsequent use must be measured against this fundamental right, too (cf. BVerfGE 100, 313 <359>; 110, 33 <68 and 69>; 113, 348 <365>). In this regard, it is also irrelevant that the aforementioned statutory provisions require that the retained data be used not by the public authorities themselves, but by private providers seeking to comply with the respective information requests received from the authorities. 195

d) Lastly, § 100g of the Code of Criminal Procedure also gives rise to an interference with Art. 10(1) of the Basic Law. It enables law enforcement authorities to compel companies obliged to retain data pursuant to § 113a of the Telecommunications Act to transfer this data to these authorities, and to subsequently use it. Thus, both § 100g(1) first sentence of the Code of Criminal Procedure itself and requests for data access based thereon constitute acts of public authority that interfere with Art. 10(1) of the Basic Law. 196

III.

Formally, there are no objections to the challenged provisions. They satisfy the requirement that interferences be based on a statutory provision in accordance with Art. 10(2) first sentence of the Basic Law, and they fall within the legislative compe- 197

tence of the Federation.

[…] 198-203

IV.

Substantively, interferences with the privacy of telecommunications are constitutional if they serve legitimate purposes in the interest of the common good and also satisfy the principle of proportionality for the rest (cf. BVerfGE 100, 313 <359>), i.e., if they are suitable, necessary and appropriate for achieving these purposes (cf. BVerfGE 109, 279 <335 *et seq*.>; 115, 320 <345>; 118, 168 <193>; 120, 274 <318 and 319>; established case-law). 204

Thus, the six-month retention of telecommunications traffic data without specific grounds, as required under §§ 113a and 113b of the Telecommunications Act, serving qualified uses in the domains of law enforcement, public security and the tasks of the intelligence services, is not *per se* incompatible with Art. 10 of the Basic Law. In enacting such a statutory framework, the legislator can pursue legitimate purposes for which the described data retention regime is a suitable and necessary means within the meaning of the principle of proportionality. Nor is such retention unjustifiable from the outset with regard to the requirement of proportionality in its strict sense. Provided that the statutory framework is designed in a way that sufficiently reflects the particular weight of the resulting interference, the retention of telecommunications traffic data without specific grounds is not necessarily subject to the strict prohibition on gathering and storing data for further retention as set out in the case-law of the Federal Constitutional Court (cf. BVerfGE 65, 1 <46 and 47>; 115, 320 <350>; 118, 168 <187>). 205

1. Increasing the effectiveness of law enforcement, public security measures and the tasks of the intelligence services are legitimate purposes, which can in principle justify an interference with the privacy of telecommunications (cf. BVerfGE 100, 313 <373, 383 and 384>; 107, 299 <316>; 109, 279 <336>; 115, 320 <345>). […] Nevertheless, precautionary data retention not based on specific grounds is only ever permissible in exceptional cases. The underlying rationale as well as the design of the relevant framework are subject to particularly strict requirements, especially regarding the purposes for which the data may be used. 206

2. The legislator may recognise the precautionary retention of telecommunications traffic data without specific grounds as a suitable means to achieve the legislative aims pursued, so as to enable a later transfer of retained data – prompted by specific grounds – to the competent authorities in the domains of law enforcement, public security or intelligence. Data retention creates investigation possibilities that, given the increasing relevance of telecommunications, also for preparing or committing criminal acts, are promising in many cases and that would not exist otherwise. […] 207

3.The legislator may also regard the retention of telecommunications traffic data for 208

a period of six months as a necessary means. Less restrictive means that would allow for similarly comprehensive investigation measures are not ascertainable. […]

4. Moreover, the retention of telecommunications traffic data for a period of six months, on the scale provided for in § 113a of the Telecommunications Act, is not from the outset disproportionate in the strict sense. 209

a) This notwithstanding, such data retention constitutes a particularly serious interference, with indiscriminate effects that are unprecedented in our legal system: throughout the entire six-month period, virtually all telecommunications traffic data of all citizens is stored, regardless of whether any culpable conduct can be attributed to them, and regardless of whether there is an – at least abstract – danger or any other qualified grounds prompting the measure. The envisaged data retention concerns everyday behaviour that is a fundamental part of our daily interactions and indispensable for social participation in modern society. […] 210

The retained data has extensive informative value. Depending on how the affected persons use telecommunications services, the data may by itself already reveal profound insights into the social environment and the individual activities of individual citizens – this applies all the more if the data serves as a starting point for further investigations. Under the telecommunications traffic data retention regime provided for in § 113a of the Telecommunications Act, only traffic data is stored (including time, duration, connections involved and – in case of mobile phones – location), but not the communication contents. However, a comprehensive and automated analysis of such data could allow considerable conclusions to be drawn about the contents of communications, including contents that fall within the intimate sphere. Where long-term monitoring takes place regarding both the participants of phone conversations (including members of certain professions, institutions or interest groups, or providers of certain services) and regarding the date, time and location of conversations, detailed conclusions can be drawn – by linking data – regarding the persons whose traffic data is analysed; these conclusions may concern social or political affiliations as well as personal preferences, interests and weaknesses of the affected persons. In this regard, no confidentiality protection is provided. Depending on telecommunications practices, and even more so in the future, such data retention may make it possible to create conclusive personality and movement profiles of virtually all citizens. In relation to groups and associations, retained data might also reveal internal influence structures and decision-making processes. 211

Data retention that makes such data uses in principle possible, and that might even be deliberately used to that end in certain cases, constitutes a serious interference. It adds to the weight of interference that, regardless of how the framework governing the use of retained data is designed, such data retention considerably increases the risk that citizens become the subject of further investigations even where they themselves did not prompt any such investigations. For example, the fact that a person happens to be within a particular cell site or is contacted by a particular person at the 212

wrong time may already suffice to subject that person to wide-ranging investigations and to the pressure of having to explain themselves. In addition, the considerable burden for the persons concerned is aggravated by the potential for abuse arising from such data collection. […] Furthermore, the retention of telecommunications data is of particular weight because the affected persons are not immediately aware of the data retention as such, nor of the intended use of the retained data; what is more, the measure also covers telecommunications undertaken with expectations of confidentiality. As a result, the retention of telecommunications traffic data without specific grounds is capable of leaving citizens with the diffuse and alarming feeling of being watched, which can impair the exercise of fundamental rights without worry or fear in many areas.

b) Even though the obligation to retain data indiscriminately affects an exceptionally large number of people, resulting in an interference of great weight, the legislator is not constitutionally barred, *per se,* from imposing an obligation to retain data for a six-month period, as provided for in § 113a of the Telecommunications Act. This notwithstanding, according to the Federal Constitutional Court's established case-law, the state is strictly barred from gathering personal data for retention, at least where such data has not been rendered anonymous and is gathered for undefined or yet to be defined purposes (cf. BVerfGE 65, 1 <46>; 100, 313 <360>; 115, 320 <350>; 118, 168 <187>). However, the precautionary retention of telecommunications traffic data without specific grounds does not necessarily constitute a form of data gathering that would fall under this absolute prohibition. Rather, where data retention actually serves defined purposes, it may satisfy the requirements of proportionality in the strict sense. Yet this requires a statutory design that adequately reflects the resulting interference (see V below). 213

aa) Firstly, it is relevant, in the present case, that the envisaged retention of telecommunications traffic data is not directly carried out by the state; rather, an obligation to retain the relevant data is imposed on private service providers. Therefore, the data is not centrally pooled at the time of retention. Instead, it is held separately by many individual companies, and is not immediately made available to the state in its entirety. In particular, the state is not granted direct access to the data, which must be ensured by appropriate statutory provisions and technical arrangements. Only in a second step may state authorities request access to the retained data, in the event that specific grounds arise; this must be further specified by criteria set out in law. In this regard, the specific design of the provisions governing requests for access to and the subsequent use of retained data can ensure that data retention is not undertaken for undefined or yet to be defined purposes. Thus, where a statutory obligation to retain data is imposed, it can, and must, also be ensured that the state may only obtain actual knowledge of the data and use it within limits set out in clear legal provisions. These limits must take into account the weight of the extensive data collection and they must restrict requests for data access and the actual data use to that part of the data that is absolutely necessary. In addition, the separation of data retention and 214

access to the data upon request structurally enhances transparency and oversight regarding data use, the details of which must be specified in statutory provisions.

bb) The six-month retention of telecommunications traffic data does not by itself negate the constitutional precepts enshrined in Art. 10(1) of the Basic Law; it neither violates the human dignity core (Art. 1(1) of the Basic Law) enshrined in Article 10(1) of the Basic Law nor the essence (*Wesensgehalt*) of this fundamental right (Art. 19(2) of the Basic Law). Although the data retention is extraordinary in scope, it is still subject to effective limitations. For instance, the retention is limited to traffic data, excluding the contents of telecommunications. In addition, the data may only be retained for a limited time period. In view of the scope and informative value of the retained data, the retention period of six months is very long and just barely within the maximum limit of what can be justified in terms of proportionality. However, citizens can trust that – except for cases where weighty grounds prompted state authorities to exceptionally request data access – their data will be deleted at the end of the retention period and that any later reconstruction is impossible. 215

cc) Nor does the six-month retention of telecommunications traffic data amount to a measure aimed at the total registration of the entire communications or activities of all citizens. Instead, the measure remains limited in scope, is informed by the special significance of telecommunications in the modern world, and reacts to the particular potential for dangers that may arise in this context. […] 216

[…] 217

Nevertheless, the retention of telecommunications traffic data must not be understood as paving the way for legislation aiming to enable, to the greatest extent possible, the precautionary retention of all data that could potentially be useful for law enforcement or public security purposes. Regardless of how the provisions governing data use were designed, any such legislation would be incompatible with the Constitution from the outset. The retention of telecommunications traffic data without specific grounds will only satisfy constitutional standards if it remains an exception to the rule. […] It is an integral part of the constitutional identity of the Federal Republic of Germany that the state may not record and register the exercise of freedoms by citizens in its entirety (cf. BVerfGE 123, 267 <353 and 354> on the guarantee of constitutional identity); it is incumbent upon the Federal Republic of Germany to ensure respect for this constitutional identity within the European and international context. With the precautionary retention of telecommunications traffic data in place, there is considerably less leeway for allowing other types of data gathering not based on specific grounds, including for measures originating at EU level. 218

dd) In summary, the six-month retention of telecommunications traffic data on the scale provided for by the legislator in § 113a(1) to (8) of the Telecommunications Act is, at present, not disproportionate from the outset. However, for it to be unobjectionable under constitutional law, it is imperative that the statutory framework governing retention and use of the data be designed in a manner that adequately reflects the 219

particular weight of such a data retention regime.

V.

The design of the statutory framework governing the precautionary retention of telecommunications traffic data, as provided for in § 113a of the Telecommunications Act, must satisfy particular constitutional requirements, especially with regard to data security, the scope of permissible data use, transparency and legal protection. The interferences resulting from such data retention are only proportionate in the strict sense if sufficiently stringent and clear statutory provisions give effect to these requirements. 220

1. The retention of telecommunications traffic data on the scale provided for in § 113a of the Telecommunications Act requires particularly high standards of data security laid down in statutory provisions. 221

In view of the scope and the potential informative value of the data sets compiled by means of such retention, data security is of great significance for the proportionality of the challenged provisions. This is particularly true because the data is retained by private service providers, which operate under the realities of profitability and cost pressure with little incentive to ensure data security. […] Thus, it is imperative that a particularly high standard of security be put in place, beyond what would normally be required under constitutional law for the storage of telecommunications data. These data security requirements apply both to the retention and to the transfer of data at the request of authorities; similarly, effective safeguards are necessary to ensure compliance with deletion requirements. 222

[…] 223

Constitutional law does not specify the necessary data security requirements in every detail. Ultimately, the adopted standard must ensure a particularly high level of security that specifically takes into account the nature of the data sets compiled by means of telecommunications traffic data retention. […] 224

It is necessary to enact a qualified statutory framework that outlines at least the basic features of such a particularly high standard of data security in a clear and binding manner. In this respect, the legislator may entrust a regulatory agency with the technical details of the required standard. However, the legislator itself must ensure that the decision as to the type and scope of the necessary data security measures is not ultimately left to the respective telecommunications providers in an unchecked manner. […] Furthermore, constitutional law requires that compliance on the part of service providers be monitored in a way that is transparent to the public and includes oversight by an independent data protection officer (cf. BVerfGE 65, 1 <46>), and that a balanced sanctions regime be put in place that attaches appropriate weight to breaches of data security. 225

2. The retention of telecommunications traffic data as provided for in § 113a of the 226

Telecommunications Act furthermore requires statutory provisions governing data use. Whether the design of this framework is proportionate determines not only the constitutionality of the respective statutory provisions on data use, which in itself constitute a separate interference with fundamental rights, but is also relevant for determining whether the data retention regime as such is constitutional. According to the case-law of the Federal Constitutional Court, the more serious the interference resulting from data retention, the more strictly the conditions and scope of data use must be defined in the underlying statutory framework. The legislator must specify precisely and clearly, for each subject matter, the grounds prompting the respective interference, its purpose and scope, as well as the threshold for exercising these powers (cf. BVerfGE 100, 313 <359 and 360>*;* 110, 33 <53>; 113, 29 <51>; 113, 348 <375>; 115, 166 <191>; 115, 320 <365>; 118, 168 <186 and 187>).

Accordingly, the use of data obtained through the systematic retention of virtually all telecommunications traffic data without specific grounds is subject to particularly strict requirements. […] Therefore, use of this data is only permissible if it serves exceptionally significant tasks aimed at the protection of legal interests, i.e. if it serves, for instance, the prosecution of criminal offences that threaten exceptionally significant legal interests or the averting of dangers to such legal interests. 227

a) In the domain of law enforcement, this means that requests for data access require at least the suspicion, based on specific facts, of a serious criminal offence. When imposing the obligation to retain data, the legislator itself must already determine definitively which criminal offences should qualify as serious. In this respect, it is afforded a margin of appreciation. The legislator may either refer to existing statutory catalogues of offences or draw up a new catalogue, for example to include criminal offences for which telecommunications traffic data is particularly relevant. However, the classification of the relevant criminal offence as serious must be objectively reflected in the definition of the crime contained in the underlying provision of criminal law, in particular by the specified range of punishment (cf. BVerfGE 109, 279 <343 *et seq*., in particular 347 and 348>). A blanket clause or mere reference to the notion of considerable criminal offences is not sufficient. 228

In addition to establishing an abstract catalogue of relevant criminal offences, the legislator must ensure that the use of the retained telecommunications traffic data is permissible only if the charges in the specific criminal case also qualify as serious (cf. BVerfGE 121, 1 <26>; on considerable criminal offences cf. BVerfGE 107, 299 <322>; on particularly serious criminal offences within the meaning of Art. 13(3) of the Basic Law, cf. BVerfGE 109, 279 <346>) and if the use of the retained data satisfies the principle of proportionality. 229

b) In the domain of averting dangers to public security, the use of retained data must also be subject to effective limitations. Here, it would not actually be a suitable legislative approach to simply make data access subject to catalogues specifying criminal offences which the envisaged data use aims to prevent (cf. BVerfGE 122, 120 230

<142>). […] Instead, a suitable approach would be for the statutory framework to directly identify the legal interests whose protection is invoked as grounds to justify the intended data use; the statutory framework should also specify the necessary level of danger to the relevant legal interests that sets the threshold for exercising these powers. Such a framework would be in keeping with the nature of public security as a regime for safeguarding legal interests meriting protection, and ensure that the interference with fundamental rights is directly connected to the aim invoked to justify it.

When balancing the weight of the interference resulting from the retention and subsequent use of data against the significance of effective public security measures, it follows that requesting access to retained telecommunications traffic data is only permissible if it serves to avert dangers to life, limb or liberty of the person, to the existence or security of the Federation or a *Land*, or to the general public (cf. BVerfGE 122, 120 <141 *et seq*.>). In this respect, the statutory basis authorising the interference must at least require factual indications of a specific danger (*konkrete Gefahr*) to the legal interests meriting protection. […] This means that there must be a situation where it is sufficiently likely, in the individual case, that certain persons will cause damage to the interests protected by the relevant statutory provision in the foreseeable future, unless the state intervenes. […] The existence of a specific danger is determined by three criteria: it concerns an individual case; it is foreseeable that the danger will result in actual damage within a certain time period; and the cause of the danger can be attributed to individual persons. Nevertheless, requests for access to retained data may already be justified at a time when it cannot be established with sufficient probability that the danger will materialise in the near future, 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 measure can be targeted at and focused on them. By contrast, the weight of interference 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. 231

c) The constitutional requirements relating to the use of retained data for maintaining public security apply to all instances where statutory provisions authorise interferences with fundamental rights to serve the aim of preventing dangers. Therefore, they also apply to the use of retained data by the intelligence services. […] 232

[…] 233

The Court is aware that, as a result of these requirements, the intelligence services will likely be excluded from using retained telecommunications traffic data in many 234

cases. Yet this follows from the nature of their tasks, which inherently concern precautionary intelligence operations; it does not, however, constitute an acceptable reason under constitutional law for relaxing the requirements which derive from the principle of proportionality for interferences of this type (cf. BVerfGE 120, 274 <331>).

d) It must also be ensured that data use remains limited to specific purposes even after the data has been requested by and transferred to the authorities; this also requires procedural safeguards. In this respect, it must be statutorily guaranteed that the data is analysed without undue delay following its transfer; where the data proves to be irrelevant to the purposes pursued, it must be deleted (cf. BVerfGE 100, 313 <387 and 388>). Moreover, it must be ensured that the data is destroyed as soon as it is no longer needed for the defined purposes, and that this is documented in the files (cf. BVerfGE 100, 313 <362>; 113, 29 <58>). 235

Telecommunications traffic data does not lose the protection afforded under Art. 10 of the Basic Law simply because one state body has already obtained knowledge of it. Therefore, the requirement deriving from this fundamental right that use of the data be clearly limited to specific purposes also applies to any subsequent sharing of this data and information with other authorities. However, this does not rule out changes in the purpose for which the data may be used. Yet a change in purpose requires a separate statutory basis, which, in turn, must also satisfy constitutional requirements (cf. BVerfGE 100, 313 <360>; 109, 279 <375 and 376>). In consequence, the legislator may only provide for the sharing of telecommunications traffic data [obtained through data retention] with other bodies if it serves tasks that would also have justified direct access to this data [by the receiving body] (cf. BVerfGE 100, 313 <389 and 390>; 109, 279 <375 and 376>; 110, 33 <73>). This must be documented by the body sharing the data (cf. BVerfGE 100, 313 <395 and 396>). Here, the required purpose limitation can only be guaranteed if the obtained data subsequently remains identifiable as data initially gathered by means of data retention. Therefore, the legislator must provide for an obligation to label this data accordingly (cf. BVerfGE 100, 313 <360 and 361>). 236

e) Finally, further constitutional limitations may arise with regard to the scope of data access that may be requested by the authorities. […] 237

In principle, the foregoing requirements already set high thresholds for the use of retained telecommunications traffic data. In light of this, the legislator is afforded leeway when further specifying the permissible scope of data use. In particular, the legislator may in principle leave the case-by-case assessment of proportionality to the judge deciding on requests for access to retained data. However, in certain cases it is constitutionally required under the principle of proportionality to recognise an absolute prohibition on granting data access to authorities, at least with respect to a narrowly-defined group of telecommunications that merit special confidentiality protection. These might include, for example, telecommunications with persons, public authorities and organisations involved in social or church work that offer counselling 238

in emotional or social crisis situations, exclusively or predominantly over the phone, to callers who generally remain anonymous, where these organisations or their staff are themselves already bound by confidentiality obligations (cf. § 99(2) of the Telecommunications Act).

3. In addition, the retention of telecommunications traffic data without specific grounds and the use of retained data are only proportionate if the legislator puts in place sufficient safeguards to ensure transparency of data use and to guarantee effective legal protection and adequate sanctions for violations. 239

a) For the use of data obtained from data retention to be unobjectionable, certain constitutional requirements, including transparency requirements, must be met. To the greatest possible extent, the use of the data must be limited to overt measures. Where this is not possible, it is in principle necessary that the affected persons be notified, at least after the measures have been carried out. If, exceptionally, not even *ex post* notification is given, a judicial decision authorising the lack of notification must be obtained. 240

aa) The retention of all telecommunications traffic data without specific grounds, for a period of six months, constitutes a serious interference, not least because it can generate the feeling of being under constant surveillance; it allows profound and unforeseeable insights into citizens' private life, while they have no immediate knowledge or awareness that their data is being accessed. The individual has no idea which state authority has what kind of information about them; what the individual does know, however, is that the authorities may have extensive and in some cases highly personal information on them. 241

This situation may instil a diffuse sense of threat in relation to data retention, which the legislator must counteract by providing for an effective transparency regime. Statutory requirements to inform the affected persons about the collection or use of their data are among the key instruments of data protection under fundamental rights (cf. BVerfGE 100, 313 <361>; 109, 279 <363 and 364>; 118, 168 <207 and 208>; 120, 351 <361 and 362>). […] Without this information, the affected persons can neither challenge the lawfulness of the authorities' use of their data nor assert possible rights to have their data deleted or rectified, or to seek satisfaction (cf. BVerfGE 100, 313 <361>; 109, 279 <363>; 118, 168 <207 and 208>; 120, 351 <361>). 242

bb) These transparency requirements include the principle of the overtness of the collection and use of personal data. Under constitutional law, the use of personal data without the knowledge of the affected person is only permissible if the purpose of the inquiry for which data access is requested would otherwise be frustrated. The legislator may in principle assume that this is the case where the pursued purpose concerns public security or the tasks of the intelligence services. By contrast, in the domain of law enforcement, it should generally be feasible to collect and use the data by means of overt measures. […] Accordingly, affected persons must in principle be notified before requests for data access or the transfer of data are carried out. Re- 243

tained data may only be used covertly if it is necessary in the individual case and authorised by a judge.

244 To the extent that the data is used covertly, the legislator must provide for a requirement to at least notify the affected person *ex post*. In this regard, it must be ensured that the persons whose data was directly targeted – regardless of whether they were classified as suspects, persons responsible for a danger to public security (*Polizeipflichtige*), or third parties – must in principle be informed, at least after the measure has been carried out. […]

245 By contrast, it is not constitutionally required to provide for similarly strict notification requirements vis-à-vis persons whose telecommunications traffic data was only incidentally obtained and who were not themselves targeted by the authorities. While the number of persons incidentally included in the analysis of telecommunications traffic data may be quite high, the mere temporary disclosure of their data to the authorities may not even leave any trace nor does it necessarily have consequences for the affected persons. […]

246 b) Moreover, the design of the statutory framework for the retention of telecommunications traffic data is only proportionate if it guarantees effective legal protection and an adequate sanctions regime.

247 aa) In order to guarantee effective legal protection, requests for access to and the transfer of this data must generally be subject to prior judicial authorisation (*Richtervorbehalt*).

248 According to the Federal Constitutional Court's case-law, investigation measures which result in serious interferences with fundamental rights require prior review by an independent authority. This applies in particular if the interference with fundamental rights is carried out covertly and cannot directly be perceived by affected persons (cf. BVerfGE 120, 274 <331>). This may be the case regarding authorities' requests for access to and the transfer of telecommunications traffic data. In view of the weight of the resulting interference, the legislator's latitude is reduced in that such measures must in principle be subject to judicial authorisation. As judges must be personally and professionally independent and are bound only by the law, they can best and most reliably ensure that the rights of the affected person are respected in the individual case (cf. BVerfGE 77, 1 <51>; 103, 142 <151>; 120, 274 <332>). Art. 10(2) second sentence of the Basic Law recognises an exception regarding oversight in relation to interferences with freedom of telecommunications by the intelligence services. Here, prior judicial review may be replaced by a review carried out by bodies or auxiliary bodies appointed by Parliament that review the specific surveillance measure in question – like a judge would – in the individual case (cf. BVerfGE 30, 1 <21>).

249 The legislator must set out the requirement of prior judicial review in specific and clear provisions combined with strict standards regarding the content and the reasons of the warrant issued by the court (cf. BVerfGE 109, 279 <358 and 359>). This also

gives rise to the requirement that requests for access to retained data themselves be sufficiently substantiated and sufficiently limited in scope, so as to enable the courts to exercise an effective review (cf. BVerfGE 103, 142 <160 and 161>). It is only on this basis that the court deciding on the request can and must assess independently whether the intended use of retained data satisfies the statutory requirements. This entails a careful examination of the statutory prerequisites applicable to the interference, including in particular the statutorily defined threshold for exercising the powers constituting interferences. When issuing the requested warrant, the court must give detailed reasons for its decision. In addition, the principle of proportionality requires that the authorised data access be clearly specified in the warrant and sufficiently selective in scope (cf. BVerfGE 103, 142 <151>), so that the service providers do not have to undertake their own substantive examination. It is only on the basis of a clear warrant that the service providers are permitted, and can be compelled, to transfer the requested data.

Effective review also entails that, based on the warrant, it is incumbent upon the telecommunications companies, in their capacity as third-party entities bound by data retention obligations, to extract and transfer the requested data so that the authorities are not given direct access. This ensures that any use of the data is dependent on the cooperation of several actors and relies on decision-making structures that are informed by mutual checks. 250

bb) It is also required under constitutional law that legal recourse be available to seek an *ex post* review regarding the use of retained data. Where affected persons did not have the opportunity to challenge the use of their telecommunications traffic data in court before the measure was carried out, they must be allowed the possibility of *ex post* judicial review. 251

cc) Finally, the design of the statutory framework is only proportionate if it sets out effective sanctions for violations of rights. If serious violations of the privacy of telecommunications were to ultimately remain without sanction, the protection of the right of personality would be eroded, given that it is non-material in nature even in its specific manifestation under Art. 10(1) of the Basic Law (cf. […] BGHZ 128, 1 <15>); this would run counter to the duty of the state to ensure that individuals can freely develop their personality (cf. BVerfGE 35, 202 <220 and 221>; 63, 131 <142 and 143>; 96, 56 <64>), and to protect them against risks to the right of personality originating from third parties (cf. BVerfGE 73, 118 <210>; 97, 125 <146>; 99, 185 <194 and 195> […]). This would in particular be the case if data obtained without authorisation could be used largely unhindered by restrictions, or if affected persons were routinely denied any satisfaction compensating the unauthorised use of their data due to lack of material damage. 252

However, in this context the legislator has broad leeway to design. […] In determining whether there is a need for more comprehensive legislation, the legislator may choose to first monitor the case-law developed by the ordinary courts under the cur- 253

rently applicable legislative framework; the legislator can thus determine whether, as the law stands, courts already give due consideration to the particular severity of the personality right violations that typically result from unauthorised access to or use of retained data, and thereby satisfy the constitutional requirements.

4. Less stringent constitutional requirements apply if the retained data is only used indirectly; this is the case where the authorities are allowed to request information on subscribers of certain IP addresses, which the service providers must then identify by using retained data. Conferring powers on the authorities to request this type of information is generally permissible to a greater extent than requests for access to and direct use of retained telecommunications traffic data by the authorities themselves; therefore, it need not necessarily be limited to narrowly-defined grounds in the form of catalogues listing criminal offences or protected legal interests. 254

a) […] 255-257

b) […] 258-260

c) Accordingly, the legislator may permit the authorities to request such information for the purposes of law enforcement, public security and the tasks of the intelligence services, where the authorities exercise general investigatory powers conferred by other legislation authorising interferences; it is not required that such information requests be subject to narrowly-defined catalogues of protected legal interests or relevant criminal offences. […] However, the applicable statutory thresholds for exercising these powers must exclude purely speculative requests for information; it must be ensured that information requests be based on a sufficient initial suspicion of criminal conduct (*Anfangsverdacht*) or sufficient facts indicating a specific danger in the individual case. In this respect, the requirement of a specific danger based on factual indications applies in all instances where the request for information is made by the intelligence services or by the authorities in charge of averting dangers to public security and order. The legal and factual basis justifying the respective request for information must be documented in the relevant files. It is, however, not necessary to make such requests for information subject to prior judicial authorisation. 261

Nevertheless, making this information available to the authorities constitutes an interference of considerable weight; therefore it would not be permissible to generally allow such information requests without any restriction, including for the purpose of prosecuting or preventing any type of administrative offence. Lifting Internet anonymity is only permissible if a protected legal interest is impaired and the legal order attaches increased weight to that interest, not just in relation to the measure at issue but also in other contexts. This does not completely rule out that information may be requested for the purposes of prosecuting or preventing administrative offences. Yet the relevant offences must not only be expressly specified by the legislator, they must also be of particular weight – including in the individual case. 262

Moreover, there is no reason to set aside the principle of transparency (see C V 3 263

above) regarding the identification of IP addresses. Affected persons may generally assume that their use of the Internet remains anonymous; therefore, they in principle have the right to be informed of the fact that, and for which reasons, this anonymity was lifted. Accordingly, the legislator must provide for a requirement to notify affected persons, unless such notification would frustrate the purpose pursued or interfere with other overriding interests of third parties or of the affected persons themselves. Where the authorities exceptionally refrain from notification in accordance with the applicable statutory provisions, the reasons must be documented in the relevant files. Yet it is not required that judicial confirmation of the decision to refrain from notification be obtained.

5. The constitutionally required guarantees of data security and of clearly defined purpose limitations on data use that satisfy proportionality requirements are inseparable elements of any statutory framework imposing obligations to retain data; enacting such guarantees is therefore incumbent upon the federal legislator as the competent authority to legislate on data retention obligations. By contrast, the legislative competence for provisions governing requests for data access by the authorities, and for specifying the applicable transparency and legal protection regime, lies with the legislator competent to legislate on the respective underlying subject matter. 264

[…] 265-268

VI.

The challenged provisions do not satisfy these requirements. This notwithstanding, § 113a of the Telecommunications Act does not conflict with the fundamental right to the privacy of telecommunications under Art. 10(1) of the Basic Law on the grounds that the scope of the data retention obligations set out in § 113a(1) to (7), (11) of the Telecommunications Act were disproportionate from the outset. Rather, the provisions on data security, on purpose limitations and transparency regarding data use, and on legal protection do not meet the constitutional requirements. In consequence, the design of the statutory framework as a whole fails to adhere to the principle of proportionality. §§ 113a and 113b of the Telecommunications Act, and § 100g of the Code of Criminal Procedure to the extent that it authorises requests for access to data retained pursuant to § 113a of the Telecommunications Act, are therefore incompatible with Art. 10(1) of the Basic Law. 269

1. The scope of § 113a of the Telecommunications Act as such does not render the provision unconstitutional. […] § 113a of the Telecommunications Act cannot be regarded as an attempt by the state to create a precautionary mechanism that generally keeps data available for law enforcement and public security purposes. Its large scope notwithstanding, § 113a of the Telecommunications Act only allows data retention in the form of a limited exception, in an attempt to respond to the particular challenges that modern telecommunications pose to law enforcement and public security. 270

2. However, the statutory framework fails to ensure the particularly high standard of data security that would be constitutionally required for a data collection of this nature. § 113a(10) of the Telecommunications Act merely provides for a general obligation to ensure, by technical and organisational measures, that the retained data can be accessed exclusively by persons who are specifically authorised; yet the provision fails to specify any further details. Other than that, the statutory framework only refers to the general duty of care incumbent upon service providers in the telecommunications sector. Hence, there is no statutory provision giving effect to the particularly strict requirements regarding data security that apply here due to the extensive scope and informative value of the data collection envisaged in § 113a of the Telecommunications Act. §§ 88 and 109 of the Telecommunications Act, which are implicitly referenced [regarding service providers' duty of care] do not sufficiently guarantee a particularly high standard of data security; given their broad scope of application, these provisions recognise various qualifying circumstances that may result in less strict standards. […] 271

[…] 272

§ 109(3) of the Telecommunications Act does not guarantee sufficient data security either. […] 273

§ 9 of the Federal Data Protection Act, in conjunction with the applicable statutory annex, cannot compensate for the lack of adequate data security standards in the Telecommunications Act. On an abstract level, this provision does contain certain high standards for data security. However, § 9 of the Federal Data Protection Act, which in any case only applies subsidiarily, […] is too general to ensure, in a sufficiently specific and reliable manner, the particularly high security standards that would be necessary in relation to the data retained pursuant to § 113a of the Telecommunications Act. 274

All in all, the particularly high standard of data security that would be necessary for the data retained pursuant to § 113a of the Telecommunications Act is not ensured by binding and clear statutory guarantees. […] The framework also lacks a balanced sanctions regime that accords at least as much weight to non-compliance with data security standards as to non-compliance with the obligation to retain data. […] 275

3. The provisions governing the transfer and use of retained data pursuant to § 113b first sentence, first half-sentence of the Telecommunications Act do not satisfy the constitutional requirements. 276

a) The provisions on the use of retained data for law enforcement purposes are already incompatible with the constitutional standards derived from the principle of proportionality. 277

aa) Use of the data retained pursuant to § 113a of the Telecommunications Act may only be allowed subject to particularly strict requirements, which § 113b first sentence no. 1 of the Telecommunications Act in conjunction with § 100g of the Code of Crim- 278

inal Procedure does not meet. […]

§ 100g(1) first sentence no. 1 of the Code of Criminal Procedure fails to ensure, both in general and in the individual case, that only serious criminal offences constitute sufficient grounds for obtaining the relevant data; it merely states – without providing an exhaustive catalogue of relevant offences – that generally any considerable criminal act provided sufficient grounds. § 100g(1) first sentence no. 2, second sentence of the Code of Criminal Procedure is even less in line with constitutional law; it recognises any criminal act committed by means of telecommunications, regardless of its seriousness and subject only to a general assessment of proportionality, as possible grounds for requesting data access. Under this provision, use of the data retained pursuant to § 113a of the Telecommunications Act could be prompted by virtually any criminal act. Given the increasing importance of telecommunications in everyday life, the use of retained data would thus no longer remain the exception. The legislator no longer limits the use of retained data to the prosecution of serious criminal offences but greatly extends its scope beyond these grounds – in doing so, the legislator also goes far beyond the objective of data retention laid down in EU law, which again is limited to the prosecution of serious criminal offences and does not even concern data retention for the purposes of averting dangers to public security. It is true that retained data could be very useful, specifically for prosecuting criminal offences committed by means of telecommunications; therefore, restricting the use of retained data may in some cases render the successful investigation of criminal offences more difficult or even impossible. However, it is inherent in the guarantee enshrined in Art. 10(1) of the Basic Law, and the corresponding requirements of proportionality, that not every measure that could be useful for law enforcement purposes, and may even be necessary in the individual case, is also permissible under constitutional law. […] 279

bb) Furthermore, § 100g of the Code of Criminal Procedure fails to satisfy the constitutional requirements in that it generally permits requests for data access without the knowledge of the affected person (§ 100g(1) first sentence of the Code of Criminal Procedure). In light of the constitutional requirements regarding transparency of data use, the data retained pursuant to § 113a of the Telecommunications Act may only be obtained covertly where this is necessary for overriding reasons, which must be specified in more detail by the legislator, and subject to judicial authorisation. 280

cc) The design of the provisions governing the notification of affected persons does also not fully satisfy the constitutional standards set out above. This notwithstanding, the envisaged scope of the notification requirement does not raise any constitutional concerns as such. […] Specifically, it is not objectionable that pursuant to § 101(4) fourth sentence of the Code of Criminal Procedure, affected persons who were not themselves targeted by the requested data access need not be notified in every case but only where a balancing of interests so indicates. This balancing of interests can and must give sufficient consideration to the interests of persons that are indirectly affected by the measure. 281

By contrast, the provisions on judicial review in cases where the authorities may refrain from notification are inadequate. § 101(6) of the Code of Criminal Procedure provides for judicial review only in cases where notification is deferred pursuant to § 101(5) of the Code of Criminal Procedure, but not in cases where notification is indefinitely refrained from pursuant to § 101(4) of the Code of Criminal Procedure. This does not sufficiently reflect the great significance of such notifications for ensuring transparent use of the data retained pursuant to § 113a of the Telecommunications Act. Where requests for data access directly target the traffic data of a specific person, refraining from *ex post* notification requires exceptional grounds, which must be reviewed by a judge. Yet no such judicial review is provided for in cases where notification is refrained from pursuant to § 101(4) third sentence of the Code of Criminal Procedure on grounds of overriding interests on the part of affected persons. 282

dd) By contrast, the challenged provisions do ensure judicial review regarding requests for data access and data use in line with the constitutional requirements. In accordance with § 100g(2) first sentence and § 100b(1) first sentence of the Code of Criminal Procedure, obtaining the data retained pursuant to § 113a of the Telecommunications Act requires a warrant issued by a judge […] 283

However, the statutory provisions on the formal requirements regarding such warrants are not sufficiently clear […] The relevant statutory provisions must at the very least require that the warrant define the scope of the data authorised for transfer in a manner that is sufficiently selective, in line with the principle of proportionality, and also unambiguous to the service providers. 284

b) The challenged provisions also fail to meet the constitutional requirements with regard to requests for access to, and the subsequent use of, data retained pursuant to § 113a of the Telecommunications Act for the purposes of public security and the tasks of the intelligence services. From the outset, the basic concept of § 113b first sentence nos. 2 and 3 of the Telecommunications Act does not satisfy the requirements concerning sufficient purpose limitations on data use. In this provision, the federal legislator merely outlines, in generalised terms, the areas of state action for which data access may be requested; however, it does not specifically delineate the purposes for which the data may be used. […] Rather, obliging service providers to retain all telecommunications traffic data while allowing the police and intelligence services to use this data in the context of almost all of their tasks leads to the creation of a data pool that is open to diverse and unlimited uses. As the data pool is not subject to limitations other than vaguely defined objectives, the federal and *Land* legislators could independently and freely grant access to this data. The establishment of such an open data pool without specific purpose limitations breaks the required link between the storage of data and the purpose for which the data is stored; this is incompatible with the Constitution […]. 285

[…] 286

c) The design of the provisions governing the use of data retained pursuant to 287

§ 113a of the Telecommunications Act is also disproportionate in that it provides absolutely no protection against the transfer of retained data relating to relationships of trust. In principle, such protection must be provided at least for a narrowly-defined group of telecommunications connections that merit special confidentiality protection […].

4. Lastly, § 113b first sentence, second half-sentence of the Telecommunications Act, which allows service providers to indirectly use data retained pursuant to § 113a of the Telecommunications Act in order to fulfil information requests pursuant to § 113(1) of the Telecommunications Act, also fails to fully satisfy the requirements of proportionality. 288

Yet by the standards set out above, it is not objectionable under constitutional law that in § 113b first sentence, second half-sentence of the Telecommunications Act, the legislator does not subject requests for information on the subscribers of certain IP addresses already known to the authorities to the particularly strict requirements that apply in relation to requests for direct access to data retained pursuant to § 113a of the Telecommunications Act. […] 289

[…] 290

However, § 113b first sentence, second half-sentence in conjunction with § 113(1) of the Telecommunications Act is too broad, in terms of proportionality, in that it generally recognises the prosecution of administrative offences as sufficient grounds justifying requests for data access. […] 291

5. In summary, neither the statutory provisions on data security nor the provisions on the use of retained data in § 113b first sentence no. 1 of the Telecommunications Act in conjunction with § 100g of the Code of Criminal Procedure, § 113b first sentence nos. 2 and 3 of the Telecommunications Act, and § 113b first sentence, second half-sentence of the Telecommunications Act meet the constitutional requirements. Consequently, the obligation to retain data pursuant to § 113a of the Telecommunications Act as such also lacks sufficient constitutional justification. The challenged provisions are therefore incompatible with Art. 10(1) of the Basic Law in their entirety. 292

VII.

[…] 293-304

VIII.

[…] 305

IX.

The violation of the fundamental right to the protection of the privacy of telecommunications under Art. 10(1) of the Basic Law renders void §§ 113a and 113b of the Telecommunications Act, as well as § 100g(1) first sentence of the Code of Criminal 306

Procedure, to the extent that these provisions allow the authorities to obtain traffic data retained pursuant to § 113a of the Telecommunications Act. The challenged provisions are therefore found to violate fundamental rights, and are declared void (cf. § 95(1) first sentence and § 95(3) first sentence of the Federal Constitutional Court Act). Accordingly, the telecommunications traffic data that was compiled by service providers at the request of authorities yet – based on the preliminary injunctions of 11 March 2008 and 28 October 2008 – was not transferred to the requesting authorities but temporarily stored instead must be deleted without undue delay. This data may no longer be transferred to the requesting authorities.

[…] 307

The decision is unanimous with regard to the questions of European law, the formal constitutionality of the challenged provisions, and the question whether the precautionary retention of telecommunications traffic data can as such be compatible with the Constitution. With regard to the finding that §§ 113a and 113b of the Telecommunications Act are unconstitutional, the decision was taken with 7:1 votes, and with regard to other questions of substantive constitutional law, as indicated in the dissenting opinions, it was taken with 6:2 votes. 308

The Court decided with 4:4 votes that the provisions must be declared void pursuant to § 95(3) first sentence of the Federal Constitutional Court Act, and not merely incompatible with the Basic Law. Thus, the general rule, as laid down in the law, on the legal consequences attached to a declaration of voidness prevails, namely that the provisions may not continue to apply, not even on a transitional basis or with a limited scope. 309

Papier Hohmann-Dennhardt Bryde

Gaier Eichberger Schluckebier

Kirchhof Masing

Dissenting Opinion of Justice Schluckebier

I can neither agree with the outcome of the decision nor with large parts of its reasoning for the following considerations. 310

The Senate majority qualifies the retention of traffic data as a particularly serious interference with the fundamental right under Art. 10 of the Basic Law. In my view, particular weight must indeed be accorded to such an interference; however, it proves to be considerably less serious than surveillance measures targeting communications contents (see I below). Furthermore, the objectives pursued by the legislator include, in particular, the investigation of crimes that, based on the circumstances of the individual case, constitute considerable crime or have been committed by means of telecommunications, and that would otherwise be difficult to investigate; in light of these objectives, I consider the interference resulting from the retention of traffic data and from the provisions on data access in criminal proceedings to be, in principle, justified under constitutional law. In my view, the provisions on which the interference is based essentially meet the requirement of proportionality in the strict sense, particularly in the assessment whether the measure is appropriate and reasonable (*zumutbar*; see II below). The provisions merely fail to satisfy the substantive requirements for ensuring data security in relation to the retention and transfer of telecommunications traffic data; in this respect, I concur with the majority of the Senate and see no need to reiterate the relevant considerations. As regards the legal consequences of the Court's decision, I believe that – even based on the constitutional assessment of the Senate majority – the challenged provisions should not have been declared void; rather, the Court should have ordered that the provisions remain applicable subject to the preliminary injunctions issued by the Court, until new provisions are enacted. 311

I.

The Senate majority considers the retention of traffic data by service providers for a period of six months to be a particularly serious interference with the fundamental right under Art. 10(1) of the Basic Law. I do not agree with this assessment. 312

The privacy of telecommunications protects against *the state obtaining knowledge* of the contents and circumstances of communications (cf. BVerfGE 100, 313 <358>; 106, 28 <37>; 107, 299 <312 and 313>). The Senate majority argues that the private service providers' obligation to retain data (§ 113a of the Telecommunications Act) amounted to an interference on the grounds that the service providers acted as "agents assisting the state", making the retention carried out by them attributable to the state. Based on this reasoning, it is particularly relevant for assessing the intensity of interference that prior to any potential data access by state authorities, the traffic data remains exclusively in the sphere controlled by the private service providers. The data is in the hands of the very party with whom a contract for telecommunications services was concluded; in this type of contractual relationship, the party using 313

the telecommunications services fundamentally trusts, based on tacit expectations, that their contractual provider will treat data originally collected for technical reasons and billing purposes with strict confidentiality, and ensure data protection in this regard. Furthermore, if an appropriate level of data security is guaranteed based on what is technologically feasible, there is no objective basis for assuming that such data retention might have a chilling effect on citizens, which would intensify the interference, or – as the Judgment puts it – create a “feeling of being under constant surveillance” and a “diffuse sense of threat”. Moreover, the data retention is not carried out covertly but on the basis of a promulgated law. The measure does not target the *contents* of telecommunications. Where the traffic data does allow, to a limited extent, to also draw conclusions on the communication contents, or even makes it possible to create movement profiles or profiles of one’s social relations, this must be taken into account in assessing the proportionality of the corresponding provisions on data access and in assessing whether the application of the law in practice meets proportionality requirements. While such uses, which are permitted based on sufficiently weighty reasons, may give rise to an intense interference in individual cases, they prove to be limited to exceptional cases overall. Thus, it is not warranted that the assessment of the data retention framework attach crucial importance to these exceptional cases or that they invariably be relied on as the starting point of the assessment.

314 […] It is true that the circumstances of the case at hand are special given the large-scale impact and the precautionary nature of the obligation to retain data. However, the weighing of the interference must still make a noticeable distinction between this type of interference and the particularly serious interferences that arise in connection with the acoustic surveillance of private homes, or the remote searches of information technology systems, but also in connection with the content-related surveillance and analysis of telecommunications *by means of direct interception by state bodies*; those cases – in contrast to the measure at hand – present a particularly high risk that the absolutely protected core of private life could be affected. The collection of the traffic data of all telecommunications is carried out by private service providers, without public authorities obtaining knowledge of the data; the possibility of the authorities to request access to the data constitutes a separate measure, which is subject to strict substantive conditions and procedural safeguards – for instance where the data is obtained by the authorities pursuant to § 100g of the Code of Criminal Procedure – and which in practice must be reviewed and authorised and must also be strictly limited in scope. From the perspective of the affected fundamental rights holders, neither data retention nor the separate possibility of requesting data access amount to an interference with fundamental rights of such weight that it could reasonably be qualified as “particularly serious”, which denotes the most severe type of interference conceivable. Ultimately, what remains is an interference that results from the retention carried out by private service providers, and that can be characterised as particularly weighty. This differentiation will become relevant in the assessment of whether the challenged provisions are appropriate [in terms of proportionality].

II.

Contrary to the Senate majority's assessment, the challenged provisions on the obligation to retain traffic data and the possibility of the authorities to obtain this data for law enforcement purposes are not inappropriate; the burdens they impose on the affected persons are reasonable and the provisions are therefore proportionate in the strict sense. 315

1. The provisions sufficiently reflect the requirement derived from the principle of proportionality that interferences be appropriate and reasonable. In an overall balancing of the severity of the interference with Art. 10(1) of the Basic Law and the weight of the reasons invoked as justification, it becomes apparent that the legislator has respected the limits set by the requirement of proportionality. 316

[…] 317

The assessment of whether the statutory framework is appropriate under constitutional law must first take into account that fundamental rights are not only defensive rights against state interference. They have an objective dimension that gives rise to the duty of the state to protect citizens against infringements. This duty of protection requires the state to take suitable measures to prevent violations of legal interests; to investigate when violations occur; to attribute liability for a violation of legal interests; and to restore the peaceful legal order (*Rechtsfrieden*) disrupted by such violations […]. In this sense, ensuring the protection of citizens and their fundamental rights and of the foundations of society, and the prevention and investigation of considerable criminal offences, are also prerequisites for peaceful coexistence and the carefree enjoyment of fundamental rights by citizens. Measures for effectively investigating criminal offences, and effectively averting dangers to public security, are therefore not *per se* a threat to the freedom of citizens; they are, however, not permissible without any restraint or limit. Rather, these measures must remain within the limits of what is appropriate and reasonable, ensuring the enjoyment of the fundamental rights as well as the protection of legal interests of the individual. In a state under the rule of law, citizens must be able to rely on effective protection *by* the state just as much as on protection *against* the state […]. Accordingly, the Federal Constitutional Court has described the state as a constituted power of peace and order; it has recognised the state's duty to guarantee the security of its citizens as a constitutional value that is equal to other constitutional values and an indispensable element for the institutional legitimation of the state (cf. BVerfGE 49, 24 <56 and 57>; 115, 320 <346>). 318

It is incumbent upon the legislator to create the necessary legal bases for investigating criminal offences and averting dangers to public security; in striking a balance between conflicting interests in this context, it must be taken into account that the individual, who is connected to and bound by the community, can be reasonably expected to tolerate certain impairments that serve the protection of other citizens' legal interests and fundamental rights, but also their own protection (cf. BVerfGE 4, 7 <15>; 33, 303 <334>; 50, 166 <175>). In view of this, the legislator must strike a bal- 319

ance, on the one hand protecting the freedoms of fundamental rights holders, while on the other hand providing an effective statutory framework for ensuring, by appropriate and reasonable means, that the legal interests and fundamental rights of citizens are protected, and criminal offences are investigated; in this respect, the legislator must be afforded leeway.

2. The legislator kept within the leeway afforded by the Constitution with regard to designing the obligation to retain telecommunications traffic data for a period of six months; the statutory provisions specifying the purposes for which retained data may be used; and the provisions permitting authorities to obtain such data in criminal proceedings. In view of the fundamental rights and legal interests these provisions seek to protect, the impairment resulting from the retention of traffic data for the affected communicating parties is neither inappropriate nor unreasonable […]. 320

a) The leeway granted to the legislator in striking an abstract balance between the respective legal interests and rights involved in the freedom and security conundrum (cf. BVerfGE 109, 279 <350>; 115, 320 <346>) is in part informed by the unique characteristics of the subject matter of the statutory framework and the realities it seeks to address. Therefore, the assessment of whether the challenged provisions are appropriate and reasonable must also take into account the aims and effectiveness of the statutory framework. 321

With the Act Revising the Law on Telecommunications Surveillance and Other Covert Investigation Measures and Transposing Directive 2006/24/EC, the legislator fundamentally reformed the system of covert investigation methods under the Code of Criminal Procedure. […] This was based on the consideration that in the present day, telecommunications traffic data is either not stored at all, or deleted before a judicial warrant authorising requests for data access can be obtained or even before the information necessary for seeking such a warrant has been ascertained; this is in part attributed to technical advances resulting in the proliferation of flat-rate contracts, which means that telecommunications traffic data is no longer available months later – as used to be the case in the past […]. Moreover, it is common knowledge that criminal acts are committed on and via the Internet. In other words, social realities, including criminal behaviour, are also reflected in the use of different types of telecommunication. […] 322

[…] 323

Under these circumstances, the legislator cannot, in principle, be barred from considering the effectiveness of the means it must provide for the purposes of protecting the legal interests of victims of crime, and from adapting to changed circumstances; this may entail imposing an obligation on service providers to store and retain traffic data in their sphere for a certain time period. […] According to the legislator's assessment, which is not objectionable, the availability of traffic data for a six-month period is of great importance for effective law enforcement and public security measures, not only regarding serious crime, but also for the investigation of crime that, based on 324

the circumstances of the individual case, concerns considerable criminal acts or criminal acts that have been committed by means of telecommunications and are difficult to investigate without access to traffic data (cf. BVerfGE 115, 166 <192 *et seq*.>; […]).

Accordingly, the Senate majority acknowledges that the increased use of electronic or digital means of communication and their advance into virtually all areas of life has created new obstacles to law enforcement and the averting of dangers to public security. The Senate majority also accepts that modern communication technologies are increasingly used for committing a wide variety of criminal acts, rendering criminal activities more effective. In my view, however, the Senate majority does not attach the necessary weight to this development in its assessment of proportionality in the strict sense. 325

b) Moreover, the Senate majority's decision effectively amounts to an almost complete reduction of the margin of appreciation and leeway afforded the legislator for enacting appropriate and reasonable statutory provisions in the domains of law enforcement and public security that serve to protect the population. Therefore, the Senate majority also fails to sufficiently take into account the requirement of 'judicial self-restraint' [English term used in the original] incumbent upon Constitutional Court Justices in relation to conceptual decisions taken by the democratically legitimated legislator. It provides step-by-step instructions to the legislator, setting out all the details of the envisaged statutory framework, without affording the legislator any margin of manoeuvre for finding a solution that, based on its own assessment, responds best to today's developments in the field of telecommunications. 326

[…] 327

3. […] 328-329

4. Finally, the Senate majority denies the legislator the possibility of allowing requests for access to traffic data in the investigation of criminal offences that are not listed in the current catalogue laid down in § 100a(2) of the Code of Criminal Procedure but that, based on the circumstances of the individual case, constitute considerable criminal acts, and of criminal acts committed by means of telecommunications (§ 100g(1) first sentence nos. 1 and 2 of the Code of Criminal Procedure). In doing so, the Senate majority also fails to sufficiently take into account the weight of these criminal offences and – to the extent that the legislator considers them difficult to investigate – the significance of the traffic data for effective criminal investigations. […] 330

According to the Senate majority, access to traffic data retained pursuant to § 113a of the Telecommunications Act should also be excluded in relation to criminal offences committed by means of telecommunications; in this respect, it fails to sufficiently take into account the legislator's assumption that these offences would otherwise be difficult to investigate. These difficulties may render requests for data access appropriate, as is the case where investigations concern criminal acts of particular 331

weight. […].

Since it is incumbent upon the legislator to guarantee effective law enforcement and to ensure that there are no substantial gaps in protection, the legislator must not be barred from granting the authorities access to traffic data also in cases where criminal acts that, while not necessarily constituting particularly serious offences, still violate legal interests of particular weight, if the legislator considers this the only way to prevent the creation of *de facto* legal vacuums where criminal investigations would largely be pointless. […] 332

[…] 333

5. Similar considerations apply with regard to the threshold set by the Senate majority for granting access to retained data for the purposes of averting dangers to public security. The legal interests recognised by the Senate majority as sufficiently weighty grounds for permitting requests for access to and the use of traffic data should have included the averting of dangers to assets of substantial value the preservation of which is in the public interest, even if the danger in question does not pose a threat to the general public. It does not seem plausible to me to exclude such assets of substantial value given that they in fact enjoy fundamental rights protection (cf. Art. 14(1) of the Basic Law). […] 334

6. Lastly, the Senate majority advocates an extension of the requirement to notify affected persons when their traffic data is accessed and demands not only that data access in criminal proceedings be, in principle, limited to so-called *overt* access, but also requires a notification "*before* requests for access to or the transfer of the data are carried out" unless such a requirement jeopardises the purpose of the investigation. This requirement, too, goes beyond the legislative concept, thereby encroaching upon the legislator's leeway to design. […] 335

III.

[…]

Schluckebier

Dissenting Opinion of Justice Eichberger

I do not fully agree with the decision of the Senate majority regarding the outcome of the decision and essential elements of its reasoning. In principle, I concur with Justice Schluckebier's criticism, and I largely agree with his conclusion and reasoning. Therefore, I will limit myself to giving a brief summary of the considerations on which my position is based: 337

1. I, too, believe that imposing a statutory obligation to retain telecommunications traffic data is a weighty interference with Art. 10(1) of the Basic Law given that its scope is broad and comprehensive in terms of persons affected and subject matters; given that the data retention is not based on specific grounds; and given that the data is retained for a considerable duration. However, since the obligation to retain data is limited to traffic data and does not concern the contents of telecommunications, and since it is carried out by private service providers in a decentralised manner, the interference arising from data retention is not of such overriding weight as the Senate majority generally assumes. In my view, the concern expressed by the Senate majority that data retention might have a chilling effect on the communication behaviour of the population is […] unfounded in light of the legislative design of the data retention framework; at any rate, there is no empirical evidence for such a chilling effect. 338

In my opinion, the major burden for citizens with regard to the legal interest protected under Art. 10(1) of the Basic Law, which results from ordering data retention, therefore lies primarily in the potential risks created by such a large data collection in terms of possible abuse by the service providers themselves or by unauthorised third parties, or of excessive use by law enforcement or police authorities. Precautions must be taken to prevent such abuse. I therefore fully agree with the view of the Senate majority concerning the stringent requirements for data security regarding the data retained by the service providers, which must be defined by law. In principle, I also agree with most of the other procedural safeguards regarding data retention, requests for data access and further data use (which concern data deletion and documentation, transparency and legal protection) which the Senate majority considers necessary; however, I find that the requirements which the Senate majority sets out for the legislator in this context are overly detailed in many respects and do not sufficiently take into account the leeway to design that the Constitution affords the legislator in this context. 339

2. Unlike the Senate majority, and concurring with Justice Schluckebier, I think that the legislative design of §§ 113a and 113b of the Telecommunications Act, which divides the legislative responsibility for imposing obligations to retain data and for authorising requests for data access, is, in principle, compatible with the Constitution. Within this legislative design, § 113b of the Telecommunications Act does not constitute a separate interference with Art. 10(1) of the Basic Law that goes beyond the obligation to retain data pursuant to § 113a of the Telecommunications Act. The provision does define the purposes for which traffic data may be retained, as required by 340

the Constitution. Only the separate statutory authorisations to request access to traffic data, envisaged by § 113b first sentence of the Telecommunications Act, result in a new interference with Art. 10(1) of the Basic Law, and the significance of this interference does go beyond that of the data retention performed pursuant to the former provision. With § 113b of the Telecommunications Act, the federal legislator leaves to federal or *Land* legislation, depending on whether the legislator of the Federation or at Land level is competent for the respective subject matter, the authority to decide, based on its constitutional and democratic legitimation, whether and to what extent access to telecommunications traffic data should be permissible for law enforcement purposes, for averting dangers to public security or for the tasks of the intelligence services. When making this decision, the respective legislator is of course responsible for respecting the constitutional boundaries of access to traffic data in line with the principle of proportionality.

341 This does not amount to an order to collect and retain data for unspecified purposes, which would be impermissible under constitutional law. In § 113a of the Telecommunications Act, the federal legislator imposed an obligation on service providers to retain data, and in § 113b of the Telecommunications Act, it specified the purposes for which the retained data may be used. I agree with the view of the Senate majority that, by ordering the data retention, the federal legislator assumed responsibility for the potential threats to citizens; this requires that at least a minimum threshold for exercising these powers be determined, in addition to the general definition of its purpose […]. However, in my opinion it is not required under constitutional law that the purposes for which the retained data may be used be already specified in a detailed and definitive manner at the time the obligation to retain data is imposed, as demanded from the federal legislator by the Senate majority.

342 3. Finally, and above all, I cannot agree with the outcome of the balancing of interests conducted by the Senate majority to the extent that it considers the use of the data retained pursuant to § 113a of the Telecommunications Act for law enforcement purposes, which is governed by § 100g of the Code of Criminal Procedure, to be unconstitutional. Firstly, this is due to the fact that, in my view, the Senate majority from the outset attaches too much weight to the interference with Art. 10(1) of the Basic Law resulting from the ordering of data retention; by contrast, it does not attach enough significance to the justified interests of the general public and of individual citizens in effective law enforcement and in effective public security. Secondly, it fails to sufficiently respect the leeway afforded the legislator in assessing the conflicting protected legal interests and in designing the statutory framework. In this respect, I agree with the remarks made by Justice Schluckebier in his dissenting opinion.

343 Another shortcoming of the proportionality assessment performed by the Senate majority is that, when balancing the conflicting interests, the Senate always assumes that the greatest possible interference will occur, namely that the data will be accessed extensively with the ultimate aim of creating movement profiles of the affected citizens or of profiling their social relations. […] However, this perspective fails to

consider that a large number of requests for data access may concern individual incidents, short time periods and the telecommunications relations of only one or few persons […]. It is obvious that the weight of interference resulting from such requests for data access is minor and cannot be compared to the weight of interference resulting from access to communication contents […]. By regarding any kind of data access as a particularly serious interference with Art. 10(1) of the Basic Law, irrespective of its specific scope in the individual case, and thus generally assuming that the legislator is constitutionally obliged to establish very high thresholds for exercising these powers, the Senate majority, in my view, is contradictory in its assessment, – even though it denies this – because the Senate majority does not object to the authorities accessing similar data if the service providers retain the data for technical reasons rather than pursuant to § 113a of the Telecommunications Act.

Based on these considerations, and regardless of the different frame of reference for the weighing of interests, I do concur with the standards developed and the requirements set by the Senate majority for permissible use of the traffic data for public security purposes and the tasks of the intelligence services (see C V 2 b and c above); however, I cannot concur with the requirements set by the Senate majority for the use of the data for law enforcement purposes (see C V 2 a and C VI 3 a, aa above). In this respect, I consider the differentiated approach to the obtaining and use of data for law enforcement purposes, as laid down by the legislator in § 100g of the Code of Criminal Procedure, to be constitutional. It is incumbent upon the judge deciding on the permissibility of a request for data access in a given case to adequately take into account the legal interests of the affected persons meriting protection under Art. 10(1) of the Basic Law and the weight of the respective interference, as the legislator specifically requires in § 100g(1) second sentence of the Code of Criminal Procedure with regard to criminal offences committed by means of telecommunications. 344

4. In my opinion, even from the Senate majority's point of view, the Court should have merely declared the challenged provisions incompatible with the Basic Law instead of void. In accordance with the preliminary injunctions issued in this matter, it should have ordered that data can be obtained and retained at least for an interim period until new provisions that are compatible with the Constitution have been enacted. Even though the Senate majority considers requests for data access which meet the requirements set out in the preliminary injunctions to be in principle constitutional, and even though it can be expected that the enactment of new provisions reflecting these requirements will follow, the Senate majority still chose to declare the challenged provisions void without a transitional period and to impose an obligation to delete the traffic data collected on the basis of the preliminary injunctions. In doing so, the Senate majority tolerates impairments of law enforcement and, above all, puts important protected legal interests in jeopardy. I cannot support this outcome. 345

Eichberger

Bundesverfassungsgericht, Beschluss des Ersten Senats vom 2. März 2010 - 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08

Zitiervorschlag BVerfG, Beschluss des Ersten Senats vom 2. März 2010 - 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08 - Rn. (1 - 345), http://www.bverfg.de/e/rs20100302_1bvr025608en.html

ECLI ECLI:DE:BVerfG:2010:rs20100302.1bvr025608