Headnotes

to the judgment of the First Senate of 2 March 2010

– 1 BvR 256/08 –

– 1 BvR 263/08 –

– 1 BvR 586/08 –

1. **Precautionary storage of telecommunications traffic data without cause for six months by private service providers as provided by Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 (OJ L 105 of 13 April 2006, p. 54; hereinafter: Directive 2006/24/EC) is not in itself incompatible with Article 10 of the Basic Law (*Grundgesetz* – GG); any potential priority of the Directive is therefore not relevant to the decision.**

2. **The principle of proportionality requires the formulation of the legislation on such storage to take appropriate account of the particular weight of the encroachment upon fundamental rights constituted by the storage. Sufficiently sophisticated and well-defined provisions are required with regard to data security, to the use of the data, to transparency and to legal protection.**

3. **The guarantee of data security and the restriction of the possible use of the data, in well-defined provisions, are, as inseparable elements of legislation creating a duty of data storage, the responsibility of the Federal legislature, under Article 73.1 no. 7 of the Basic Law. In contrast, the responsibility for creating the retrieval provisions themselves and for drafting the provisions on transparency and legal protection depends on the legislative competence for the respective subject-matter.**

4. **With regard to data security, there is a need for statutory provisions which lay down a particularly high security standard in a well-defined and legally binding manner. It must be ensured by statute, at all events fundamentally, that this standard is oriented to the state of development of the discussion between specialists, constantly absorbs new knowledge and insights and is not subject to a free weighing of interests against general business considerations.**

5. **The retrieval and the direct use of the data are only proportionate if they serve overridingly important tasks of the protection of legal interests. In the area of the prosecution of criminal offences, this requires the suspicion of a serious criminal offence based on specific facts. For warding off danger and for performing the duties of the intelligence services, they may only be permitted if there is actual evidence of a concrete danger to the life, limb or freedom of a person, to the existence or the security of the Federation or of a *Land* or to ward off a danger to public safety.**

6. **A merely indirect use of the data by the telecommunications service providers to issue information with regard to the owners of Internet Protocol addresses is permissible, even independent of restrictive lists of legal interests or criminal offences, for the prosecution of criminal offences, for warding off danger and for carrying out intelligence-services duties. For the prosecution of regulatory offences, such information can only be allowed to be given in cases of particular weight expressly named by the legislature.**

FEDERAL CONSTITUTIONAL COURT

– 1 BvR 256/08 –

Pronounced

– 1 BvR 263/08 –

– 1 BvR 586/08 –

on 2 March 2010

Kehrwecker

Amtsinspektor

Registrar

of the Court Registry

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaints

I.

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

– authorised representative: Mr. Meinhard Starostik, lawyer
Schillstraße 9, 10785 Berlin –

against §§ 113a and 113b of the Telecommunications Act (*Telekommunikationsgesetz – TKG*) as amended by the Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation and for the Implementation of Directive 2006/24/EC (*Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG)* of 21 December 2007 (Federal Law Gazette (*Bundesgesetzblatt* – BGBl) I 2007, p. 3198)

– 1 BvR 256/08 –,

II.

1. of Dr. Dr. h.c. H…,
2. of Dr. S…,
3. of Ms L…,
4. of Mr. B…,

5. of Ms P…,
6. of Mr. K…,
7. of Dr. L…,
8. of Dr. W…,
9. of Prof. Dr. S…,
10. of Ms S…,
11. of Mr. F…,
12. of Mr. S…,
13. of Mr. V…,
14. of Mr. W…,

– authorised representative: Dr. Dr. h.c. Burkhard Hirsch, lawyer,
Rheinallee 120, 40545 Düsseldorf –

against the Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation and for the Implementation of Directive 2006/24/EC of 21 December 2007 (Federal Law Gazette I p. 3198)

– 1 BvR 263/08 –,

III.

1. of Ms A…,
2. of Ms B…,
3. of Mr. B…,
4. of Ms B…,
5. of Ms B…,
6. of Mr. B…,
7. of Mr. D…,
8. of Dr. D…,
9. of Dr. E…,
10. of Mr. F…,
11. of Mr. G…,
12. of Ms G…,
13. of Ms H…,
14. of Ms H…,
15. of Ms H…,
16. of Mr. H…,
17. of Mr. H…,
18. of Mr. W…,
19. of Mr. W…,

20. of Mr. T…,
21. of Dr. T…,
22. of Mr. S…,
23. of Dr. S…,
24. of Ms S…,
25. of Ms S…,
26. of Ms S…,
27. of Ms S…,
28. of Ms P…,
29. of Mr. N…,
30. of Mr. N…,
31. of Ms M…,
32. of Mr. M…,
33. of Ms M…,
34. of Ms L…,
35. of Ms K…,
36. of Mr. K…,
37. of Mr. K…,
38. of Ms K…,
39. of Ms K…,
40. of Dr. H…,
41. of Ms H…,
42. of Ms H…,
43. of Ms H…,

– authorised representative: Prof. Dr. Jens-Peter Schneider,
Lürmannstraße 10, 49076 Osnabrück –

against the provisions on data retention in the Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation and for the Implementation of Directive 2006/24/EC of 21 December 2007 (Federal Law Gazette I p. 3198)

– 1 BvR 586/08 –

the First Senate of the Federal Constitutional Court,

with the participation of

Justices Papier (President),

Hohmann-Dennhardt,

Bryde,

Gaier,

Eichberger,

Schluckebier,

Kirchhof, and

Masing

issued the following

Judgment

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

7. **§§ 113a and 113b of the Telecommunications Act as amended by the Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation and for the Implementation of Directive 2006/24/EC of 21 December 2007 (Federal Law Gazette part I 2007, p. 3198) infringe Article 10 subsection 1 of the Basic Law and are hence void.**

8. **§ 100g subsection 1 sentence 1 of the Code of Criminal Procedure (*Strafprozessordnung* – StPO) as amended by Article 1 number 11 of the Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation and for the Implementation of Directive 2006/24/EC of 21 December 2007 (Federal Law Gazette part I page 3198) infringes Article 10 subsection 1 of the Basic Law to the extent that it permits the collection of traffic data stored pursuant to § 113a of the Telecommunications Act and is void to that extent.**

9. **The telecommunications traffic data collected on the basis of the temporary injunction issued on 11 March 2008 in the proceedings 1 BvR 256/08 (Federal Law Gazette part I page 659), repeated and extended by an order of 28 October 2008 (Federal Law Gazette part I page 2239), last repeated by an order of 15 October 2009 (Federal Law Gazette part I page 3704) by providers of publicly available telecommunications services under requests for information made by competent authorities, but provisionally not transmitted to the requesting authorities, which are stored, must be deleted without delay. They may not be transmitted to the requesting agencies.**

10. **The Federal Republic of Germany is ordered to reimburse the complainants their necessary costs in the constitutional complaint proceedings.**

Reasons:

A.

The subject-matter of the constitutional complaints are provisions of the Telecommunications Act (hereinafter: TKG) and of the Code of Criminal Procedure (hereinafter: StPO) that provide a precautionary storage for six months of telecommunications traffic data by the providers of publicly available telecommunications services and the use of such data. 1

I.

The challenged provisions were inserted or amended by the Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation and for the Implementation of Directive 2006/24/EC of 21 December 2007 (Federal Law Gazette I p. 3198; hereinafter: Act for the Amendment of Telecommunications Surveillance (*Gesetz zur Neuregelung der Telekommunikationsüberwachung*)); pursuant to its Article 16.1, they have entered into force on 1 2

January 2008. They serve to implement 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).

1. All constitutional complaints directly challenge §§ 113a and 113b TKG, which have been inserted into the Telecommunications Act by Article 2 no. 6 of the Act for the Amendment of Telecommunications Surveillance. Apart from this, the constitutional complaints in the proceedings 1 BvR 263/08 and 1 BvR 586/08 directly challenge § 100g StPO as amended by Article 1 no. 11 of the Act for the Amendment of Telecommunications Surveillance to the extent that it permits the collection of data stored pursuant to § 113a TKG. 3

a) § 113a TKG aims, with regard to all publicly available telecommunications services, at storing, for six months, traffic data which provide information on the lines involved in a telecommunications connection and about the time and the locations at which an act of telecommunication has taken place and to keep them available for the state's performance of its duties. In doing so, the Act takes up demands which had been made by the Bundesrat for an extended period of time (see Bundestag printed paper (*Bundestagsdrucksache* – BTDrucks) 14/9801, p. 8; Bundesrat printed paper (*Bundesratsdrucksache* – BRDrucks 755/03 (resolution), p. 33 et seq.; BRDrucks 406/1/04; BRDrucks 406/04 (resolution); BRDrucks 723/05 (resolution), p. 1), with which the German Bundestag concurred in 2006, making reference to the respective initiatives on the European level. The German Bundestag requested the Federal Government to approve the draft Directive 2006/24/EC and to immediately submit a draft of an implementing Act (see Bundestag printed papers 16/545, p. 4; 16/690, p. 2; Minutes of plenary proceedings of the Bundestag (BTPlenarprotokoll) 16/19, p. 1430). The Federal Government complied with the request by submitting the draft Act for the Amendment of Telecommunications Surveillance (see Bundestag printed paper 16/5846). 4

§ 113a.1 sentence 1 TKG obliges the of publicly available telecommunications services to store, for a period of six months, the telecommunications service data listed in § 113a.2 to 113a.5 regarding fixed network, internet and mobile communications, the transmission of text, multi-media and similar messages, email connections and Internet access. According to § 113a.1 sentence 2 TKG, a person who provides such services without himself creating traffic data shall ensure that the data are stored, and shall inform the Federal Network Agency (*Bundesnetzagentur*) as to who is storing these data. Apart from this, a person who provides telecommunications services and in doing so alters the information to be stored pursuant to § 113a TKG is obliged to store the original and the new information. According to § 113a.11 TKG, the data are to be deleted within one month after the end of the storage period. Pursuant to § 113a.8 TKG, the contents of the communication and data on Internet sites visited may not be stored. As regards data security, § 113a.10 TKG makes reference to the care necessary in the area of telecommunications and demands that access to the stored data be exclusively possible to persons specifically authorised for this purpose. 5

Apart from data storage according to § 113a TKG, the providers of telecommunications services retain, pursuant to § 96 TKG, the possibility of storing and using telecommunications data to the extent necessary for the purposes specified therein. After the end of a telecommunications connection, these data may essentially be used pursuant to § 96.2 sentence 1 to the extent that this is necessary for charging and invoicing the parties (§ 97.1 sentence 1 TKG), for itemised billing (§ 99.1 sentence 1 TKG), to the extent necessary for recognising, locating or eliminating faults or deficiencies of telecommunications equipment (§ 100.1 TKG), and to give information about the owners of lines from which threatening or malicious calls have been made (§ 101.1 sentence 1 TKG). 6

§ 113a TKG reads as follows: 7

§ 113a 9

Duties to store data

(1) A person who provides publicly available telecommunications services for end users shall store traffic data produced or processed by him in the use of his service pursuant to subsections 2 to 5 for six months in Germany or in another Member State of the European Union. A person who provides publicly available telecommunications services for end users without himself creating or processing traffic data shall ensure that the data are stored pursuant to sentence 1 above, and shall inform the Federal Network Agency at its request as to who is storing these data. 10

(2) The providers of publicly available telephone services store: 11

1. the telephone number or other identification of the calling and called line, and in the case of call transfer or forwarding of every additional line involved, 12

2. the beginning and the end of the connection, with date and time and stating the relevant time zone, 13

3. in cases in which different services may be used as part of the telephone service, information on the service used, 14

4. in the case of mobile telephone services in addition: 15

a) the International Mobile Subscriber Identities of the calling and called lines, 16

b) the International Mobile Equipment Identity of the calling and called terminal device, 17

c) the identification of the radio cells used by the calling and the called lines at the beginning of the connection, 18

d) in the case of prepaid anonymous services, in addition the initial activation of the service, with date, time and identity of the radio cell, 19

5. in the case of Internet telephone services, in addition the Internet Protocol address of the calling and the called lines. 20

Sentence 1 applies with the necessary modifications to the transmission of a text, multi-media or similar message; in this case, in place of the information under sentence 1 no. 2, the times of the sending and the receipt of the message shall be stored. 21

(3) The providers of electronic mail services store: 22

1. when a message is sent, the identity of the electronic mailbox, the Internet Protocol address of the sender and the identity of the electronic mailbox of every receiver of the message, 23

2. when a message is received in an electronic mailbox, the identity of the electronic mailboxes of the sender and the receiver of the message and the Internet Protocol address of the sending telecommunications equipment, 24

3. in the event of access to the electronic mailbox, the identification of the mailbox and the Internet Protocol address of the person retrieving, 25

4. the points of time of the uses of the service set out in nos. 1 to 3 above with date and time, stating the relevant time zone. 26

(4) The providers of Internet access services store: 27

1. the Internet Protocol address allocated to the subscriber for use of the Internet, 28

2. a clear identification of the access line through which the use of the Internet is made, 29

3. the beginning and the end of the use of the Internet from the allocated Internet Protocol address with date and time, stating the relevant time zone. 30

(5) To the extent that providers of telephone services store or record the traffic data named in the present provision for the purposes set out in § 96.2 even if the call is not answered or is unsuccessful as the result of a network management intervention, the traffic data shall also be stored pursuant to the present provision. 31

(6) A person who provides telecommunications services and in doing so alters the information to be stored pursuant to the present provision shall store the original and the new information and the time of the alteration of this information with date and time, stating the relevant time zone. 32

(7) A person who operates a mobile telephone network for the public shall also retain, in addition to the identities of the radio cells stored pursuant to the present provision, data which reveal the geographic locations of the radio antennae supplying each radio cell and their main beam direction. 33

(8) The contents of the communication and data on Internet sites visited may not be stored under the present provision. 34

(9) The storage of the data under subsections 1 to 7 above shall be effected in such a way that requests for information made by the agencies entitled may be responded to without delay. 35

(10) The provider with obligations under the present provision shall observe the care necessary in the area of telecommunications with regard to the quality and the protection of the traffic data stored. In this connection it must ensure by technical and organisational measures that access to the stored data is exclusively possible to persons specifically authorised by it for this purpose. 36

(11) The provider with obligations under the present provision shall delete or ensure the deletion of the data stored solely pursuant to the present provision within one month after the end of the period stated in subsection 1. 37

b) § 113b TKG sets out the purposes for which the data stored pursuant to § 113a TKG may be used. In doing so, it distinguishes between transmission to authorities in order to make it possible for them to use the data to perform their duties, and use by the telecommunications service providers themselves in order to give information pursuant to § 113 TKG, in particular about the owners of Internet lines. 38

aa) § 113b sentence 1 half-sentence 1 TKG sets out the purposes for which the telecommunications enterprises may transmit the data to public authorities. The prerequisites under which such authorities, for their part, may use the data are intended to be provided in provisions under Federal or *Land* (state) law of the respective area of non-constitutional law. § 113b sentence 1 half-sentence 1 TKG provides that the provider obliged to store data may transmit the data stored solely pursuant to the duty of retention under § 113a to the competent agencies exclusively for the prosecution of criminal offences (no. 1), to ward off substantial dangers to public security (no. 2) and to perform intelligence-service duties (no. 3). 39

Pursuant to § 113b sentence 1 half-sentence 1 TKG, data may be transmitted to the respective competent authorities at their request only if this is explicitly provided in the relevant statutory provisions of non-constitutional law referring to § 113a and the transmission has been ordered in the individual case. 40

The basis under non-constitutional law for the authorisation to use the data stored pursuant to § 113a TKG for the prosecution of criminal offences is § 100g StPO, which is challenged in the proceedings 1 BvR 263/08 and 1 BvR 586/08. As regards the warding off of dangers and the intelligence services' performance of their duties, § 20m of the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz* , hereinafter: BKAG) as amended by the Act on Prevention by the Federal Criminal Police Office of Threats from International Terrorism (*Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das* 41

Bundeskriminalamt) of 25 December 2008 (Federal Law Gazette I p. 3083) and various provisions under *Land* law meanwhile make reference to § 113a TKG and thus make it possible for the competent authorities to avail themselves of the data stored according to this provision.

42 However, it was possible even before the entry into force of § 113a TKG to consult telecommunications traffic data stored in a permissible manner for the prosecution of criminal offences, to ward off danger or to perform intelligence-service duties. For example, § 100g.1 StPO as amended by Article 1 of the Act Amending the Code of Criminal Procedure (*Gesetz zur Änderung der Strafprozessordnung*) of 20 December 2001 (Federal Law Gazette I p. 3879; hereinafter: § 100g StPO, old version) provided for an obligation of the service providers to give information on telecommunications connection data, on the basis of a judicial order, where there was a suspicion of a criminal offence of substantial importance or of a criminal offence committed by means of a telecommunications terminal device. In the same manner, for example Article 34b.2 no. 1 of the Act on the Duties and Competences of the Bavarian State Police (*Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei* (Bavarian Police Duties Act – *Polizeiaufgabengesetz* ; hereinafter: BayPAG)) as amended by the Act Amending the Bavarian Police Duties Act and the Parliamentary Control Panel Act (*Gesetz zur Änderung des Polizeiaufgabengesetzes und des Parlamentarischen Kontrollgremium-Gesetzes*) of 24 December 2005 (Bavarian Law and Ordinance Gazette (GVBl) p. 641) or § 8a.1 sentence 1 no. 4 of the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz* (Federal Act on Protection of the Constitution –*Bundesverfassungsschutzgesetz* ; hereinafter: BVerfSchG) as amended by the Act Amending the Counter Terrorism Act (*Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes*) of 5 January 2007 (Federal Law Gazette I p. 2) provided authorisations to retrieve information on existing telecommunications connection data to ward off danger or to perform duties of the authority for the protection of the constitution.

43 bb) It is true that § 113b.1 half-sentence 2 TKG excludes, in principle, the use of the data stored pursuant to § 113a TKG for other purposes than those mentioned in § 113b sentence 1 half-sentence 1 TKG. However, it admits of an exception to the effect that they may also be used by the service providers to give information pursuant to § 113 TKG.

44 § 113.1 TKG permits authorities to retrieve what is known as customer and contract data pursuant to §§ 95 and 111 TKG, in particular of telephone numbers, line identifications and names and addresses of line owners. § 113b 1 half-sentence 2 TKG thus makes it possible for the service providers to give information concerning the owners of what is known as “dynamic” Internet protocol addresses (hereinafter: IP addresses). According to the present state of development, IP addresses are, as a general rule, not permanently assigned to a line as so-called “static” IP addresses but are only assigned to the respective Internet user as dynamic IP addresses for the duration of the respective access to the Internet. Information about the owner of a line from which a particular dynamic IP address has been used at a particular point in time can therefore only be given if the traffic data can be evaluated which provide information about the line to which the IP address in question was assigned at the material time. This is made possible by § 113b sentence 1 half-sentence 2 TKG with regard to the data stored according to § 113a TKG.

45 According to the prevalent view, traffic data were permitted to be used to give information about the owners of dynamic IP addresses pursuant to §113.1 TKG even before the entry into force of §§ 113a and 113b TKG (see for example Stuttgart Regional Court (*Landgericht* – LG), order of 4 January 2005 – 13 Qs 89/04 –, *Neue Juristische Wochenschrift* – NJW 2005, p. 614 (614-615); Hamburg Regional Court, order of 23 June 2005 – 1 Qs 43/05 –, *MultiMedia und Recht* – MMR 2005, p. 711 (712-713); Sankol, MMR 2006, p. 361 (365); a different view is held by the Bonn Regional Court, order of 21 May 2004 – 31 Qs 65/04 –, *Datenschutz und Daten* – DuD 2004, p. 628 (628-629); the Karlsruhe Higher Regional Court (*Oberlandesgericht* – OLG), judgment of 4 December 2008 – 4 U 86/07 –, MMR 2009, p. 412 (413-414);

Bär, *Handbuch zur EDV-Beweissicherung* , 2007, p. 148, marginal no. 212; Bock, in: Geppert/Piepenbrock/Schütz/Schuster, *Beck'scher Kommentar zum TKG* (commentary), 3rd ed. 2006, *§ 113* , marginal nos. 23-24). However, only traffic data stored pursuant to § 96 TKG could be used. The possibility of identifying the owner of a dynamic IP address via information according to § 113.1 TKG therefore depended on whether such data were still stored at the point in time of the request for information.

The identification of the owner of an IP address is of significance for example for copyright protection. If the copyright owners succeed in identifying the IP addresses under which copyright violations are committed in the Internet, the criminal prosecution authorities can identify, by means of a request for information pursuant to § 113.1 TKG, the owners of the respective lines, against whom the copyright owners can bring civil action after inspecting the files of the criminal proceedings. It is true that § 101.2 sentence 1 no. 3 of the Copyright Act (*Urheberrechtsgesetz* – UrhG) as amended by Article 6 no. 10 of the Law on the Improved Enforcement of Intellectual Property Rights (*Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums*) of 7 July 2008 (Federal Law Gazette I p. 1191) now grants persons whose copyright has been violated also a civil-law right to information vis-à-vis the telecommunications service providers. Pursuant to § 101.9 of the Copyright Act, the latter may give the information on the basis of a court order also by using telecommunications traffic data. It is, however, excluded to use the data stored pursuant to § 113a TKG (see Frankfurt am Main Higher Regional Court, order of 12 May 2009 – 11 W 21/09 –, MMR 2009, p. 542 (544), with further references; Hoeren, *Neue Juristische Wochenschrift* 2008, p. 3099 (3101); Bäcker, in: Rensen/Brink, *Linien der Rechtsprechung des Bundesverfassungsgerichts* , 2009, p. 99 (111-112), footnote 49). 46

Information pursuant to § 113.1 sentence 1 TKG is to be given to the extent necessary for prosecuting criminal or regulatory offences, to ward off dangers to public security or public order or for performing intelligence-service duties. 47

cc) § 113b TKG reads:

§ 113b 50

Use of the data stored pursuant to § 113a

The provider with obligations under § 113a may transmit the data stored solely pursuant to the duty of retention under § 113a 51

1. for the prosecution of criminal offences, 52

2. to ward off substantial dangers to public security, or 53

3. to perform the statutory duties of the authorities of the Federation and the *Länder* (states) for the protection of the constitution, of the Federal Intelligence Service (*Bundesnachrichtendienst*) and of the Military Counterintelligence Service (*Militärischer Abschirmdienst*) 54

to the competent agencies at their request, to the extent that this is provided for in the relevant statutory provisions referring to § 113a and the transmission has been ordered in the individual case; it may not use the data for other purposes, with the exception of giving information pursuant to § 113. § 113.1 sentence 4 applies with the necessary modifications. 56

The provision of § 113 TKG to which § 113b TKG makes reference reads in part:

§ 113 57

Preparation by hand of information 58

(1) Any person who, in a business capacity, provides telecommunications services or assists in providing such services shall in the individual case give, without delay, information to the competent agencies at their request about the data collected 59

> pursuant to §§ 95 and 111 to the extent that this is necessary for the prosecution of criminal or regulatory offences, to ward off dangers to public security or order or to perform the statutory duties of the authorities of the Federation and the *Länder* for the protection of the constitution, of the Federal Intelligence Service and of the Military Counterintelligence Service. The person obliged to give information pursuant to sentence 1 shall give information about data which protect the access to terminal devices or to storage systems employed in such devices or in the network, in particular PINs or PUKs, on the basis of a request for information made pursuant to § 161.1 sentence 1, § 163.1 of the Code of Criminal Procedure, to the provisions on data collection of the police laws of the Federation or of the *Länder* to ward off dangers to public security or order, to § 8.1 of the Federal Act on Protection of the Constitution, to the relevant provisions of the *Land* Acts on Protection of the Constitution, to § 2.1 of the Federal Intelligence Service Act or § 4.1 of the Military Counterintelligence Service Act; these data may not be transmitted to other public or non-public agencies. Access to data which are subject to the secrecy of telecommunications is only possible under the prerequisites of the statutory provisions which are relevant in this respect. The person obliged to give information shall observe secrecy about the provision of information towards his customers and towards third parties.

(2) … 60

c) § 100g.1 sentence 1 StPO provides for the collection of telecommunications data for purposes of the prosecution of criminal offences. According to the provision, the criminal prosecution authorities can in the first instance access traffic data which the telecommunications enterprises have stored on the basis of § 96 TKG; this was already possible according to § 100g StPO, old version. Apart from this, § 100g StPO now also permits the collection of the data stored by way of precaution pursuant to § 113a TKG. This is challenged by the constitutional complaints in the proceedings 1 BvR 263/08 and 1 BvR 586/08. 61

In detail, § 100g.1 sentence 1 StPO permits the criminal prosecution authorities, with reference to § 113a TKG to collect traffic data without the knowledge of the person concerned to the extent that this is necessary for the investigation of the facts or the establishment of the whereabouts of the suspect. This, however, only applies if specific facts create the suspicion that a person, as perpetrator or accessory, has committed a criminal offence that even in an individual case is of substantial importance, in particular a criminal offence listed in § 100a.2 StPO, or has committed a criminal offence preparatory thereto or, as perpetrator or accessory, has committed an offence by means of telecommunications. 62

Pursuant to § 100g.2 sentence 1 in conjunction with § 100b.1 sentences 1 and 2 StPO, the data collections may only be ordered by a judge unless in case of imminent danger. According to § 100g.2 sentence 1 in conjunction with § 100a.3 StPO, the order may only be directed against the accused or against persons of whom it must be assumed due to specific facts that they receive or transmit specific messages directed to the accused or originating from him or that the accused uses their line. 63

In case of offences committed by means of telecommunications, the collection of traffic data is, pursuant to § 100g.1 sentence 3 StPO, permissible only if the investigation of the facts or the establishment of the whereabouts of the suspect would be impossible in another way and the collection of the data is in a reasonable proportion to the importance of the matter. The legislature regarded this restriction as necessary for reasons of proportionality because it took the view that all in all, the intensity of the encroachment resulting from the collection of traffic data had increased due to the expansion of the data volume in connection with the obligation to store data pursuant to § 113a TKG (see Bundestag printed paper 16/5846, p. 52). 64

Pursuant to § 101.4 sentence 1 StPO, the person affected by measures according to § 100g.1 sentence 1 StPO shall be notified of them. The person affected may apply for the judicial review of such measures within two weeks following their notification (§ 101.7 sentence 2 StPO). In certain cases, notification may be dispensed with (§ 101.4 StPO), in other cases it may be deferred (§ 101.5 StPO). Unlike the dispensation of notification pursuant to § 101.4 StPO, a long-term deferral according to § 101.5 StPO requires the approval of the court. 65

§ 100g StPO reads as follows: 66

§ 100g 67

(1) If specific facts create the suspicion that a person, as perpetrator or accessory, 68

1. has committed a criminal offence that even in an individual case is of substantial importance, in particular a criminal offence listed in § 100a.2 above, or, in cases in which attempt constitutes an offence, has attempted to commit such an offence, or has committed a criminal offence preparatory thereto or 69

2. has committed an offence by means of telecommunications, 70

then, even without the knowledge of the person concerned, traffic data (§ 96.1 and § 113a of the Telecommunications Act) may be collected to the extent that this is necessary for the investigation of the facts or the establishment of the whereabouts of the suspect. In the case of sentence 1 no. 2, the measure is permissible only if the investigation of the facts or the establishment of the whereabouts of the suspect would be impossible in another way and the collection of the data is in a reasonable proportion to the importance of the matter. The collection of location data in real time is permissible only in the case of sentence 1 no. 1. 71

(2) § 100a.3 and § 100b.1 to § 100b.4 sentence 1 apply with the necessary modifications. Notwithstanding § 100b.2 sentence 2 no. 2, in the case of a criminal offence of substantial importance it is sufficient to adequately determine the place and time of the telecommunications if the investigation of the facts or the establishment of the whereabouts of the suspect in another way would be impossible or considerably more difficult. 72

(3) If the collection of traffic data is not made on the responsibility of the telecommunications service provider, then after the end of the communications process it is governed by the general provisions. 73

(4) In accordance with § 100b.5, a summary of measures under subsection 1 shall be prepared annually; this shall state: 74

1. the number of proceedings in which measures under subsection 1 have been taken; 75

2. the number of orders for measures under subsection 1, classified according to original orders and renewal orders; 76

3. the criminal offence that occasioned the order in each case, classified according to subsection 1 sentence 1 nos. 1 and 2; 77

4. the number of past months for which the traffic data under subsection 1 was requested, starting at the time when the order was made; 78

5. the number of measures that have produced no results because the data retrieved were in whole or in part not available. 79

2. Directive 2006/24/EC of the European Parliament and of the Council, whose implementation the challenged provisions serve to the extent that they concern the prosecution of criminal offences, was adopted by the Council on the basis of Article 95 EC against the votes of Ireland and Slovakia (see Council document 6598/06 ADD 1 of 27 February 2006, p. 4), after the European Parliament had rejected an initiative for a Draft Framework Decision (see Council document 8958/04 of 28 April 2004) by the French Republic, Ireland, Sweden and Great Britain on the retention of telecommunications data which relied on Article 31.1 letter c and Article 34.2 letter b of the Treaty on European Union in its version applicable until the entry into force of the Treaty of Lisbon (hereinafter: Treaty on European Union, old version) (see European Parliament document P 6 TA[2005]0348). 80

a) The Directive takes up the considerations that telecommunications traffic data are a valuable tool in the prosecution of criminal offences, in particular in the areas of organised crime and terrorism (see Recitals 7 to 10 of Directive 2006/24/EC) and that several Member States have adopted legislation providing for the retention of such data whose provisions vary considerably (see Recital 5 of Directive 2006/24/EC). It works on the assumption that the legal and technical differences created thereby present obstacles to the internal market for electronic telecommunications, since service providers are faced with different requirements regarding the types of data to be retained and the periods of retention (see Recital 6 of Directive 2006/24/EC). 81

b) The validity of Directive 2006/24/EC is doubted regarding its compatibility with the fundamental rights of the European Community (see Klesczewski, in: *Festschrift für Gerhard Fezer zum 70. Geburtstag* , 2008, p. 19 (24-25); Klug/Reif, *Recht der Datenverarbeitung* – RDV 2008, p. 89 (91 et seq.); Rusteberg, *Verwaltungsblätter für Baden-Württemberg – VBlBW* 2007, p. 171 (176); Westphal, *Europäische Zeitschrift für Wirtschaftsrecht* – EuZW 2006, p. 555 (558 -559); Zöller, *Goltdammer's Archiv für Strafrecht* – GA 2007, p. 393 (410 et seq.); Advocate General Kokott, opinion delivered on 18 July 2007 – Case C-275/06 –, ECR 2008, I-271 (276), marginal no. 82 – Promusicae –) as well as regarding the foundation on which the European Union bases its competence (see Gitter/Schnabel, *MultiMedia und Recht* 2007, p. 411 (412-413); Jenny, *Computer und Recht* – CR 2008, p. 282 (285); Klesczewski, in: *Festschrift für Gerhard Fezer zum 70. Geburtstag* , 2008, p. 19 (22 et seq.); Klug/Reif, RDV 2008, p. 89 (91); Leutheusser-Schnarrenberger, *Zeitschrift für Rechtspolitik* – ZRP 2007, p. 9 (11 et seq); Rusteberg, VBlBW 2007, p. 171 (173-174); Westphal, EuZW 2006, p. 555 (557-558); Zöller, GA 2007, p. 393 (407-408)). 82

By its judgment of 10 February 2009, the Court of Justice of the European Communities rejected an action for annulment under Article 230 EC brought by Ireland (see ECJ, judgment of 10 February 2009 – Case C-301/06 –), which relied on the main or predominant purpose of the Directive being to facilitate the prosecution of criminal offences and its only permissible legal base therefore being the provisions of the EC Treaty, old version, on police and judicial cooperation, which require unanimity, in particular Article 30, Article 31.1 letter c and Article 34.2 letter b of the EC Treaty, old version (see action of 6 July 2006 – Case C-301/06 –, OJ C 237 of 30 September 2006, p. 5). In its judgment, the Court of Justice explicitly stated that the action did not relate to any possible infringement of fundamental rights of the Community (see ECJ, judgment of 10 February 2009 – Case C-301/06 –, marginal no. 57). 83

c) According to Article 1.1 of Directive 2006/24/EC, the Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of telecommunications data, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. On the occasion of the adoption of the Directive, the Council declared that in defining "serious crime", the Member States shall have due regard to the crimes listed in Article 2.2 of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JI) (OJ L 190 of 18 July 2002, p. 1) and crime involving telecommunication (see Council document 6598/06 ADD 1, p. 4). The Directive does not contain provisions on the use of the data for duties involving the warding off of dangers or intelligence-service duties. 84

Pursuant to Article 3.1 of Directive 2006/24/EC, Member States shall ensure that the data specified in Article 5 of Directive 2006/24/EC are retained; according to Article 6 of Directive 2006/24/EC, periods of not less than six months and not more than two years from the date of the communication are to be set down. Pursuant to Article 4 of Directive 2006/24/EC, Member States shall ensure that the data retained are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State. 85

Article 7 of Directive 2006/24/EC obliges the Member States to ensure that certain minimum requirements as to data security are respected with regard to the data being retained. Apart from this, the provisions of Directives 95/46/EC and 2002/58/EC are fully applicable (see Recitals 15 and 16 of Directive 2006/24/EC). According to Article 8 of Directive 2006/24/EC, the Member States shall ensure that the data retained and any other necessary information can be transmitted upon request to the competent authorities without undue delay. Pursuant to Article 13 of Directive 2006/24/EC, the Member States shall furthermore ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under Directive 2006/24/EC. The Directive does not make provision on who is to cover the costs of data storage. 86

3. Furthermore, § 100g StPO is significant for the Convention on Cybercrime of the Council of Europe (Federal Law Gazette II p. 1242; hereinafter: Convention on Cybercrime) (see Federal Law Gazette 16/5846, pp. 27-28 and 50). The Convention not only establishes an obligation to adopt substantive criminal law in order to fight cybercrime but also an obligation to adopt specific provisions under the law of criminal procedure. In particular, according to Article 16 of the Convention, the competent authorities must be enabled to order the expeditious preservation of traffic data. It must be made possible to oblige persons who are in control of such data to preserve and maintain the integrity of those computer data at short notice to enable the competent authorities to seek their disclosure (so-called quick freeze). The legislature, however, regarded it as dispensable to adopt a provision to this effect because the data to be frozen had to be retained anyway due to the comprehensive storage ordered pursuant to § 113a TKG (see Bundestag printed paper 16/5846, p. 53). 87

4. By its order of 11 March 2008, the Federal Constitutional Court, upon the application made by the complainants in the proceedings 1 BvR 256/08, issued a temporary injunction according to which § 113b sentence 1 no. 1 TKG may only be applied in a restricted manner until the decision in the main action (see Decisions of the Federal Constitutional Court (*Entscheidungen des Bundesverfassungsgerichts* – BVerfGE 121, 1). By its order of 28 October 2008, it extended the temporary injunction to the effect that until the decision in the main action, also § 113b sentence 1 nos. 2 and 3 TKG could only be applied with restrictions (see BVerfGE 122, 120). Apart from this, the Federal Government was ordered to report [to the Federal Constitutional Court] for consecutive periods of several months on the practical effects of the data retention measures provided in § 113a TKG and of the temporary injunction on the prosecution of criminal offences. The Federal Government complied with this order with regard to the periods lasting from 1 May 2008 to 31 July 2008, from 1 August 2008 to 1 March 2009 and from 1 March 2009 to 1 September 2009. 88

II.

1. The complainants in the proceedings 1 BvR 256/08 challenge §§ 113a and 113b TKG. They challenge the violation of Article 10.1, Article 12.1, Article 14.1, Article 5.1 and Article 3.1 GG. In the proceedings conducted under the case number 1 BvR 508/08, approximately 34,000 other complainants concurred with this, making the same submissions. 89

[…] 90-116

2. The complainants in the proceedings 1 BvR 263/08 challenge not only §§ 113a and 113b TKG but also § 100g StPO to the extent that it concerns the collection of the data stored pursuant to § 113a TKG. They challenge a violation of Article 1.1, Article 2.1 in conjunction with Article 1.1, Article 10.1 and Article 19.2 GG. 117

[…] 118-133

3. The complainants in the proceedings 1 BvR 586/08 also challenge §§ 113a and 113b TKG and § 100g StPO. They challenge the violation of Article 10.1 and Article 2.1 in conjunction with Article 1.1 GG. 134

[…] 135-145

III.

Opinions on the constitutional complaints were submitted by the Federal Government, the Federal Administrative Court (*Bundesverwaltungsgericht*), the Federal Court of Justice (*Bundesgerichtshof*), the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) and, on behalf of the commissioners for data protection of the *Länder* , by the Commissioner for Data Protection and Freedom of Information of the *Land* Berlin. 146

1. The Federal Government regards the constitutional complaints as inadmissible in part, at any rate as unfounded. 147

[…] 148-164

2. The Federal Administrative Court considers the challenged provisions an encroachment upon Article 10.1 GG whose justification is doubtful. […] 165

3. Through the Chairman of its First Criminal Senate and one of the pretrial judges, the Federal Court of Justice points out that to date in the case of criminal offences committed by means of telecommunications, data which would have allowed an identification of the perpetrator had normally already been deleted when the request for information was made. […] 166

4. The Federal Commissioner for Data Protection and Freedom of Information regards the storage of data without cause pursuant to § 113a TKG as unconstitutional. […] 167

[…] 168-170

5. The Commissioner for Data Protection and Freedom of Information of the *Land* Berlin considers the essence of the secrecy of telecommunications violated by §§ 113a and 113b TKG. […] 171

6. The experts Ms Constanze Kurz, Prof. Dr. Felix Freiling, Prof. Dr. Andreas Pfitzmann, Prof. Dr. Alexander Roßnagel, Prof. Dr. Christoph Ruland, the Federal Commissioner for Data Protection and Freedom of Information, the Commissioner for Data Protection and Freedom of Information of the *Land* Berlin, the Federal Ministry of Justice assisted by the Federal Ministry of Economics and Technology and by the Federal Ministry of the Interior, the complainants in the proceedings 1 BvR 256/08 and 1 BvR 263/08 as well as the Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), the Verband der deutschen Internetwirtschaft e.V. (eco) and the Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V. (VATM) have made statements regarding technical, factual and legal questions of the Court. They concerned the telecommunications traffic data, the persons obliged to perform data retention, the crimes committed by means of telecommunications, the giving of information pursuant to § 113 TKG, the securing of the retained data against unauthorised access and the possible legal provisions on the use of such data. In the drafting of the opinion by the Federal Ministry of Justice, the Federal Network Agency (*Bundesnetzagentur*) cooperated via the Ministry of Economics and Technology; the Federal Criminal Police Office (*Bundeskriminalamt*); the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*) and the Federal Public Prosecutor General (*Generalbundesanwältin*) cooperated through the Federal Ministry of the Interior. 172

7. Apart from this, opinions were submitted by the Verband der Anwender geschäftlicher Telekommunikation e.V. (TELECOM e.V.), the Börsenverein des Deutschen Buchhandels e.V. and the Bundesverband Musikindustrie e.V. 173

IV.

In the oral hearing, statements were made by: the complainants, the Federal Government, the Federal Criminal Police Office, the Federal Network Agency, the Government of the Free State of Bavaria, the Federal Commissioner for Data Protection and Freedom of Information, the Commissioner for Data Protection and Freedom of Information of the *Land* Berlin; as experts, Prof. Dr. Dr. h.c. Hans-Jörg Albrecht, Ms Constanze Kurz, Prof. Dr. Felix Freiling, Prof. Dr. Andreas Pfitzmann, Prof. Dr. Alexander Roßnagel, Prof. Dr. Christoph Ruland, the Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), the Verband der deutschen Internetwirtschaft e.V. (eco), the Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V. (VATM), the Börsenverein des Deutschen Buchhandels e.V. and the Bundesverband Musikindustrie e.V. were heard. 174

B.

The constitutional complaints are admissible. 175

I.

1. The complainants admissibly challenge a violation of Article 10.1 GG. They use different telecommunications services such as in particular telephone services, electronic mail and Internet services for private and business purposes, and they put forward that the storage and intended use of their connection data violates their fundamental right to respect of the secrecy of telecommunications. As Article 10.1 GG also protects the confidentiality of the circumstances of acts of telecommunication (see BVerfGE 67, 157 (172); 85, 386 (396); 120, 274 (307); established case-law), such a violation by the challenged provisions is possible. 176

The challenged provisions also affect the complainants directly, personally and presently. It is true that the obligation to store data under § 113a TKG does not address the complainants, who are affected as users, but the service providers. The latter, however, are unconditionally obliged, without any margin for decision, to store the complainants' data (see BVerfGE 107, 299 (313-314)). § 113a TKG thus directly and presently results in the storage of data of the complainants for the purposes provided for in § 113b sentence 1 TKG. 177

It also cannot be maintained that the complainants are not affected directly and personally with regard to § 113b TKG und § 100g StPO merely because the provisions only have an effect on the basis of further acts of execution and because it is not yet certain whether and to what extent data of the complainants will be affected. If the person affected does not gain knowledge of the acts of execution, it is sufficient to submit that he or she will with some probability be affected by such measures. What is decisive in this context is whether the measures have a wide range and can cover third parties incidentally (see BVerfGE 109, 279 (307-308); 113, 348 (363); 120, 378 (396-397)). Accordingly, the complainants have sufficiently shown that they are personally and directly affected. With regard to the considerable length of storage of six months, and the wide range of the collected data, it is not improbable that the transmission and the use of the data according to § 113b TKG and § 100g StPO also affects persons who have not given occasion to such measures. Statements by which the complainants themselves would have to charge themselves with a criminal offence are thus not necessary to substantiate their being personally affected (see BVerfGE 109, 279 (308); 113, 348 (363); 120, 378 (396-370)). They also do not have to state that they are responsible for substantial dangers to public security or engage in activities that affect the duties of the intelligence services. 178

2. The constitutional complaint of the fourth complainant in the proceedings 1 BvR 256/08 is also admissible with regard to Article 12.1 GG to the extent that it is directed against the technical and financial burdens which result from the duties of storage. As the provider of an anonymisation service, which also operates a publicly accessible server, the complainant is in principle submitted to the duties under § 113a TKG, without indemnification or compensation being provided for this. As sanctions of administrative fines exist for non-observance of these duties (see § 149.1 no. 36, 149.2 TKG), it is also unreasonable to expect the complainant to first await acts of execution, while infringing § 113a TKG in the meantime, and then to seek recourse before the non-constitutional courts against such acts (see BVerfGE 81, 70 (82)). Thus, the complainant is itself affected directly and presently as regards its occupational freedom, 179

II.

The constitutional complaints are not inadmissible to the extent that the challenged provisions have been enacted implementing Directive 2006/24/EC. 180

The Federal Constitutional Court, however, in principle does not exercise its jurisdiction to decide on the applicability of Community law, now Union law, that is relied on as a legal basis for any acts of German courts or authorities by German courts and authorities in the sovereign territory of the Federal Republic, and does not review such legislation by the standard of fundamental rights contained in the Basic Law, as long as the European Communities (or today the European Union), in particular the case-law of the European Court of Justice, generally ensure effective protection of fundamental rights which is to be regarded as substantially similar to the protection of fundamental rights required unconditionally by the Basic Law, and in so far as they generally safeguard the essential content of fundamental rights (see BVerfGE 73, 339 (387); 102, 147 (162-163)). These principles also apply to domestic legal provisions that implement mandatory requirements of a directive in German law. Constitutional complaints which challenge the application of European Union law which is binding in this sense are in principle inadmissible (see BVerfGE 118, 79 (95); 121, 1 (15)). 181

However, the complainants can rely on the fundamental rights contained in the Basic Law to the extent that the legislature has discretion regarding the implementation of European Union law, i.e. that the legislature's action is not determined by European Union law (see BVerfGE 121, 1 (15)). Apart from this, the present constitutional complaints are also admissible to the extent that the challenged regulations are based on provisions of the Directive which have a mandatory character. The complainants assert that Directive 2006/24/EC lacks a competence basis in Community law and that it infringes European fundamental rights guarantees. They therefore seek *inter alia* a referral by the Federal Constitutional Court to the European Court of Justice so that the latter may, by means of a preliminary ruling according to Article 267 TFEU (formerly Article 234 TEC), declare the Directive void and thus open the way for a review of the challenged regulations against the standard of the German fundamental rights; they were not able to assert this before the non-constitutional courts because their constitutional complaints directly challenged the implementing Act. At any rate, a review of the challenged regulations against the standard of the fundamental rights contained in the Basic Law according to the relief sought by the complainants is not excluded from the outset. 182

C.

The constitutional complaints are essentially well-founded. The challenged provisions violate the complainants' fundamental right under Article 10.1 GG. A referral to the European Court of Justice is out of the question, since any potential priority of Community law is not relevant. The constitutional guarantees of the Basic Law are not an obstacle to an implementation – in a different form – of Directive 2006/24/EC. 183

The constitutional complaint of the fourth complainant in the proceedings 1 BvR 256/08 is unfounded to the extent that it challenges a violation of Article 12.1 GG. 184

I.

The constitutional complaints give no occasion for referral for a preliminary ruling before the European Court of Justice under Article 267 of the Treaty on the Functioning of the European Union. It is true that such proceedings instituted by the Federal Constitutional Court (see BVerfGE 37, 271 (282)) might particularly come into consideration when it is necessary to answer questions on the interpretation or the validity of Community or European Union law, which has priority over domestic law and whose implementation the Federal Constitutional Court in principle does not review by the yardstick of the fundamental rights of the Basic Law. However, such a referral is only admissible and appropriate when the crucial factor is the interpretation or validity of European Union law. That is not the case here. 185

The validity of Directive 2006/24/EC and a priority of Community law over German fundamental rights which might possibly result from this are not relevant to the decision. The contents of the Directive leave to the Federal Republic of Germany a broad discretion in shaping the storage of telecommunications traffic data for which it provides. The Directive imposes on the Member States an obligation to require the operators of publicly accessible electronic communications networks and communications services to store virtually all telecommunications traffic data for a period of at least six months (Articles 1, 3, 5 and 6 Directive 2006/24/EC). But in doing this, its provisions are essentially limited to the duties of storage themselves, and do not govern access to the data or the use of the data by the Member States' authorities. In particular, they harmonise neither the issue of access to data by the national authorities competent for criminal prosecution nor the issue of the use and the exchange of those data between those authorities (cf. ECJ, judgment of 10 February 2009 – C-301/06 –, 83). Proceeding on the basis of the minimum requirements of the Directive (Articles 7 and 13 Directive 2006/24/EC), it is also for the Member States to take the necessary measures to guarantee data security, transparency and legal protection. 186

With these contents, the Directive can be implemented in German law without violating the fundamental rights of the Basic Law. The Basic Law does not prohibit such storage in all circumstances. On the contrary, even independent of any priority of Community law, it may permissibly be ordered in compliance with the fundamental rights enshrined in the Basic Law (see IV below). A review of the challenged provisions as a whole by the yardstick of German fundamental rights is therefore not in conflict with Directive 2006/24/EC, and therefore the validity and priority of the latter is not relevant. 187

II.

The challenged provisions encroach upon Article 10.1 GG. 188

1. Article 10.1 GG guarantees the secrecy of telecommunications, which protects the incorporeal transmission of information to individual recipients with the aid of telecommunications traffic (see BVerfGE 106, 28 (35-36); 120, 274 (306-307)) against the taking of notice by state authority (see BVerfGE 100, 313 (358); 106, 28 (37)). In this connection, this protection does not only relate to the contents of the communication. On the contrary, the protection also covers the confidentiality of the immediate circumstances of the process of communication, which include in particular whether, when and how often telecommunications traffic occurred or was attempted between what persons or telecommunications equipment (see BVerfGE 67, 157 (172); 85, 386 (396); 100, 313 (358); 107, 299 (312-313)); 115, 166 (183); 120, 274 (307)). 189

The protection of Article 10.1 GG applies not only to the first access by which state authority takes notice of telecommunications events and contents. Its protective effect also extends to the information and data processing procedures which follow the taking of notice of protected communications events, and to the use that is made of the knowledge obtained (see BVerfGE 100, 313 (359)). An encroachment upon fundamental rights includes every taking of notice, recording and evaluation of communications data, and every analysis of their contents or other use by state authority (see BVerfGE 85, 386 (398); 100, 313 (366); 110, 33 (52-53)). The recording of telecommunications data, their storage, their comparison with other data, their evaluation, their selection for further use or their transmission to third parties are therefore 190

each an individual encroachment upon the secrecy of telecommunications (see BVerfGE 100, 313 (366-367)). Consequently, an order to communications enterprises to collect and store telecommunications data and to transmit them to state agencies is in each case an encroachment upon Article 10.1 GG (see BVerfGE 107, 299 (313)).

191 The right arising from Article 2.1 in conjunction with Article 1.1 GG to informational self-determination does not apply in addition to Article 10 GG. In relation to telecommunications, Article 10 GG contains a special guarantee which overrides the general provision and which gives rise to special requirements for the data that are obtained by encroachments upon the secrecy of telecommunications. In this context, however, the requirements which the Federal Constitutional Court has developed from Article 2.1 in conjunction with Article 1.1 GG may largely be transferred to the more special guarantee of Article 10 GG (see BVerfGE 100, 313 (358-359)).

192 2. a) The storage of telecommunications traffic data imposed on the service providers under § 113a.1 TKG encroaches upon the secrecy of telecommunications. In the first instance, this applies to the duties of storage relating to telecommunications services under § 113a.2 to 113a.5 TKG and in conjunction with this under § 113a.6 and § 113a.7 TKG. The information to be stored under this provision indicates whether, when, where and how often connections were established or there was an attempt to establish connections between what telecommunications installations. In particular, this also applies to the storage of data in the service of electronic mail under § 113a.3 TKG, whose confidentiality is also protected by Article 10.1 GG (see BVerfGE 113, 348 (383); 120, 274 (307)). The fact that it is technologically easy to intercept emails does not alter their confidential character and their need for protection. In this connection, storage of the data relating to the Internet connection under § 113a.4 TKG is also an encroachment upon Article 10.1 GG. Internet access enables not only communication between individuals, which is protected by the secrecy of telecommunications, but also participation in mass communication. But since it is not possible to distinguish between individual and mass communication without referring to the contents of the information transmitted in each case, which is contrary to the protective function of the fundamental right, the very storage of the data relating to the Internet access as such is to be seen as an encroachment, even if they do not contain information on the Internet pages visited (see Gusy, in: v. Mangoldt/Klein/Starck, *GG,* vol. 1, 5th ed. 2005, *Art.10* , marginal no. 44; Hermes, in: Dreier, *GG,* vol. 1, 2nd ed. 2004, *Art. 10* , marginal no. 39).

193 The encroaching nature of § 113a TKG is also not called into question by the fact that the storage prescribed by this provision is made not by the state itself, but by private service providers. For these service providers are merely used by the state authorities as helpers to carry out their duties. § 113a TKG obliges the private communications enterprises to store data solely in order to carry out the tasks of state authorities for purposes of the prosecution of criminal offences, the warding off of danger and the performance of intelligence tasks under § 113b TKG. Under these provisions, the state directly orders the impairment of fundamental rights associated with the storage, and the enterprises with a duty of storage have no room for manoeuvre in this connection; the data are to be stored in such a way that requests for information from the public authorities entitled under § 113a.9 TKG can be complied with without delay. Under these conditions, the storage of the data is to be legally attributed to the legislature as a direct encroachment upon Article 10.1 GG (see BVerfGE 107, 299 (313-314)).

194 b) The provisions on data transmission in § 113b sentence 1 half-sentence 1 TKG also constitute encroachments upon fundamental rights in Article 10.1 GG. Admittedly, in itself this provision does not permit a use of the data stored under § 113a TKG, but refers to further statutory retrieval provisions which are to be separately created. However, it does contain the fundamental specification of the purposes for which the data may be used. In this respect, it releases the telecommunications enterprises from the duty of confidentiality to which they are otherwise subject. Ultimately, the final overall regulation of the use of the data is created only by the graduated meshing of provisions on various levels of legislation, but this does not alter the fact that the definition of the purposes of use and the permission to transmit data are part of the regulation of use and thus have the nature of an encroachment. Here too it is irrelevant that §

113b TKG relates to transmission of the data by private service providers. The transmission provided for is based on a statutory arrangement and therefore directly on an act of state authority, which under Article 1.3 GG is bound by fundamental rights, requires a sovereign order in the individual case, and is made to authorities. It is therefore to be seen in law as an encroachment by the state.

c) § 113b sentence 1 half-sentence 2 in conjunction with § 113.1 TKG also creates an encroachment upon Article 10.1 GG. It provides that authorities may demand from the service providers information on contract and customer data under §§ 95, 111 TKG; the service providers can only determine these by using the data stored under § 113a.4 TKG. Independently of the question as to whether and how far information under § 113 TKG is in general an encroachment upon Article 10.1 GG or whether fundamentally it is only the right to informational self-determination under Article 2.1 in conjunction with Article 1.1 GG that is affected here, at all events information under § 113b sentence 1 half-sentence 2, § 113.1 TKG is certainly an encroachment upon the secrecy of telecommunications of Article 10.1 GG. For the provision relates to the use of the data which are stored under § 113a TKG and thus acquired by an encroachment upon Article 10.1 GG. Every following use of data which were once obtained in the form of an encroachment upon Article 10.1 GG must always be measured against this fundamental right (see BVerfGE 100, 313 (359); 110, 33 (68-69)); 113, 348 (365)). Here too it must be immaterial that this use, provided by statute, is made not by state authority itself, but by private suppliers, complying with the request for information. 195

d) Finally, § 100g StPO is also an encroachment upon Article 10.1 GG. It enables the criminal prosecution authorities to have the data stored under § 113a TKG transmitted to themselves by the persons obliged to store them, and to use these data. § 100g.1 sentence 1 StPO itself and the exercise of this authorisation, therefore, as acts of public authority, also encroach upon the area of protection of Article 10.1 GG. 196

III.

Formally, there are no objections to the challenged provisions. They fulfil the requirement of a statutory basis under Article 10.2 sentence 1 GG, and they fall under a competence of the Federation. 197

1. Under Article 10.2 sentence 1 GG, restrictions of the secrecy of telecommunications may be imposed only on the basis of a statute. Firstly, there are no doubts in this connection with regard to § 113b TKG and § 100g StPO, which – if necessary in conjunction with other provisions – are a statutory basis for individual judicial orders, on the basis of which access to the data takes place. § 113a TKG is also constitutionally unobjectionable in this respect; for the storage of data, it does not refer to individual judicial orders but directly orders storage itself. Article 10.2 sentence 1 GG also does not prevent restrictions of the secrecy of telecommunications that are made directly by statute (see BVerfGE 85, 386 (396 et seq.)). 198

2. The Federation does not lack legislative competence. The legal basis of §§ 113a, 113b TKG is Article 73.1 no. 7 GG; that of § 100g StPO is Article 74.1 no. 1, Article 72.1 GG. 199

However, Article 73.1 no. 7 GG only directly authorises legislation on the technical aspect of the installation of a telecommunications infrastructure and of the transmission of information with the aid of telecommunications equipment. This Article does not cover provisions which are focused on the contents transmitted or the nature of the use of the telecommunications (see BVerfGE 113, 348 (368); 114, 371 (385)) and which, for example, provide for telecommunications surveillance for the purpose of acquiring information for tasks of criminal prosecution or warding off danger. With regard to legislative competence, each such provision is to be assigned to the area of law for whose purposes the surveillance is provided (see BVerfGE 113, 348 (368)). 200

However, §§ 113a and 113b TKG, as part of the provisions on data protection law, are also, by virtue of a factual connection, covered by the competence to pass telecommunications legislation. In the absence of express assignment of competence, the law of data protection is fundamentally in the competence of the *Länder* . But by virtue of a factual connection, the Federal legislature is competent to legislate on data 201

protection, in that the Federation cannot sensibly legislate on a subject-matter allocated to it for legislation without legislating on the data protection provisions at the same time (see BVerfGE 3, 407 (421); 98, 265 (299); 106, 62 (115); 110, 33 (48); established case-law; on data protection law see Simitis, in: Simitis, *BDSG* , 6th ed. 2006, *§ 1* , marginal no. 4). This is the case with regard to §§ 113a, 113b TKG. These sections are connected to the provisions of the Telecommunications Act on data protection, and linked to the law on the technical conditions of the transmission of information they regulate the requirements to be observed in each case for handling the data created or processed in the provision of telecommunications services. They therefore link directly to facts that fall under the area of legislation of telecommunications. On account of this close connection between the technical transmission process and the data arising in this process, the necessary data-protection legislation for their use may only be passed uniformly by the Federal legislature, which has the competence to legislate on the transmission process. Otherwise there would be the danger that the technical and data-protection provisions on data processing would diverge, and this would be incongruous. Accordingly, in addition to the provisions of §§ 113a and 113b TKG and on the secrecy of telecommunications in §§ 88 et seq. TKG, the Telecommunications Act also contains, in §§ 91 to 107 TKG, extensive provisions on data protection that are specific to this area; as far as can be seen, their lawfulness from the point of view of competence has to date not seriously been called into question.

202 The scope of its competence allows the Federation to pass the provisions necessary to create legislation on the use of the data which is in conformity with fundamental rights. In particular, it may draft the provisions which are necessary in order that the data storage provided for in § 113a TKG and the transmission of the data to criminal prosecution authorities, authorities competent to ward off danger, and to intelligence services and the use of the data to issue information under § 113 TKG comply with the constitutional standards of Article 10.1 GG. Since it is a requirement of encroachments upon Article 10.1 GG that their purpose is determined in an area-specific and precise manner and is contained in well-defined provisions (see BVerfGE 100, 313 (359-360); 110, 33 (53); 115, 320 (365); 118, 168 (187-188)), this implies the competence to pass legislation on the purpose of the storage that is area-specific and precise and consists of well-defined provisions. However, in this connection the legislative competence of the Federation only extends as far as is required under data-protection aspects and the associated constitutional requirements. The Federation may therefore not base the authorisations for data retrieval itself on Article 73.1 no. 7 GG. It needs a separate legal basis for this, or else it must leave the decision on it to the *Länder* .

203 §§ 113a, 113b TKG fundamentally take this into consideration. They are exclusively restricted to creating the conditions for access to the data by the state through storage duties and provisions on transmission. But filling in the details is left to separate provisions on data retrieval. Notwithstanding the question of substantive law as to whether the Federation has sufficiently restricted the purposes of use here (see below C V 5 and VI 3 b), there are no objections to this on the grounds of competence.

IV.

204 The encroachments upon the secrecy of telecommunications are substantively constitutional if they serve legitimate purposes in the public interest and apart from this comply with the principle of proportionality (see BVerfGE 100, 313 (359)), i.e., are suitable, necessary and appropriate to fulfil the purposes (see BVerfGE 109, 279 (335 et seq.); 115, 320 (345); 118, 168 (193); 120, 274 (318-19)); established case-law).

205 Storage of telecommunications traffic data without cause for six months for qualified uses in the course of prosecution, the warding off of danger and intelligence service duties, as is provided by §§ 113a, 113b TKG, is therefore not in itself incompatible with Article 10 GG. The legislature may in such a provision pursue legitimate purposes to attain which such storage is suitable and necessary within the meaning of the principle of proportionality. Nor is such storage unjustifiable from the outset in relation to proportionality in the narrow sense. If legislation is drafted in a way that takes sufficient account of the encroachment

contained in this, storage of telecommunications traffic data without cause is not as such automatically covered by the strict prohibition of data retention within the meaning of the case-law of the Federal Constitutional Court (see BVerfGE 65, 1 (46-47). 115, 320 (350); 118, 168 (187)).

1. Making criminal prosecution, warding off danger and performing the tasks of the intelligence service more effective is a legitimate purpose, which can in principle justify encroachment upon the secrecy of telecommunications (see BVerfGE 100, 313 (373, 383-384); 107, 299 (316); 109, 279 (336); 115, 320 (345)). In this connection, the fact that the telecommunications traffic data are to be secured without cause by way of precaution does not automatically constitute an illegitimate objective which cancels the very principle of liberty of Article 10.1 GG. Article 10.1 GG does not prohibit every collection and storage of data whatsoever, but gives protection against a disproportionate organisation of such data collections, and in this connection in particular against boundary-expanding objectives. Only the precautionary storage of personal data for purposes that are indefinite and cannot yet be determined is strictly prohibited (see BVerfGE 65, 1 (46); 100, 313 (360)). However, only exceptionally is the precautionary storage of data permissible. Both its justification and its formulation, in particular also with regard to the envisaged purposes of use, are subject to especially strict requirements. 206

2. The legislature may regard as suitable to obtain its objective a precautionary storage of telecommunications traffic data without cause for later transmission with cause to the authorities responsible for criminal prosecution or warding off danger or to the intelligence services. This creates possibilities of detection which would otherwise not exist and in view of the increasing importance of telecommunications are promising in many cases also for the preparation and commission of criminal offences. It is irrelevant whether the provisions created by the legislature are capable of seamlessly reconstructing all telecommunications connections. Even though such a storage of data cannot ensure that all telecommunications connections can reliably be assigned to specific users, and it may be possible for criminals to circumvent storage by using Wi-Fi hotspots, Internet cafés, foreign Internet telephone services or prepaid mobile telephones registered under a false name, this cannot be cited to show that such a provision is not suitable. Suitability does not demand that the goal of the legislation is actually attained in every single case, but merely requires that the attainment of the goal is facilitated (see BVerfGE 63, 88 (115); 67, 157 (175); 96, 10 (23); 103, 293 (307)). 207

3. The legislature may also treat a six-month storage of the telecommunications traffic data as necessary. There are no less drastic means apparent that would enable similarly broad detection possibilities. In particular, the procedure known as data preservation or quick freeze is inferior with regard to effective detection; in this, the general storage of telecommunications data without cause is replaced by storage only in the individual case, which is not ordered until the date when there is concrete cause for it, for example on the basis of a particular suspicion of a criminal offence. Such a procedure, which can only cover data from the time before they were ordered to be stored if they are still available, is not as effective as continuous storage, which guarantees the existence of a complete set of data for the last six months. 208

4. Nor is storage of telecommunications traffic data for six months to an extent as provided in § 113a TKG disproportionate in the narrow sense from the outset. 209

a) Admittedly, such storage constitutes a particularly serious encroachment with a broader range than anything in the legal system to date: throughout the whole six-month period, virtually all telecommunications traffic data of all citizens are stored, without a connection to culpable conduct attributable to them, or to a dangerous situation – even a merely abstract one –, or to a situation otherwise qualified. This storage relates to everyday actions which are a basic part of day-to-day interaction and which are now indispensable for taking part in social life in the modern world. Fundamentally, no form of telecommunications is as a matter of principle excluded from storage. Admittedly, the provision ultimately leads to occasional gaps, which prevent every telecommunications connection without exception from being reconstructed with individual details, for example in certain circumstances in the use of Wi-Fi hotspots, complex private networks or service providers outside the EU. However, this does not give the 210

citizen a regular possibility of avoiding storage. Instead, the legislature attempts fundamentally to provide for all telecommunications connections in such a way that the users can be determined as extensively as possible.

211 The informative value of these data is extremely broad. Depending on the use of the telecommunications services by the persons affected, a high degree of knowledge of the social environment and the individual activities of each citizen may be obtained even from the data themselves – and all the more if the data are used as starting points for further investigations. Admittedly, storage of telecommunications traffic data, as provided for in § 113a TKG, records only the connection data (time, duration, connections involved and – in the case of mobile telephony – location), but not in addition the contents of the communication. However, it is possible to draw conclusions with regard to contents that extend into the private sphere even from these data, if they are subjected to comprehensive and automated analysis. If recipients (the particular occupational groups, institutions or interest groups they belong to or the services they offer), dates, times and places of telephone conversations are observed for a long period of time, then in combination they permit detailed conclusions on social or political affiliations and personal preferences, inclinations and weaknesses of the persons whose connection data are analysed. There is no protection of confidentiality in this connection. Depending on the use of the telecommunications, and in future with increasing frequency, such storage can make it possible to create meaningful personality profiles and mobility profiles of virtually all citizens. In relation to groups and associations, the data also, in certain circumstances, may make it possible to reveal internal influence structures and decision-making processes.

212 Storage which fundamentally makes such uses possible and in particular cases is intended to make them possible constitutes a serious encroachment. In this connection, it is also significant that, independent of a legislative approach to the use of data of whatever nature, the risk of citizens considerably increases of being exposed to further investigations without themselves having given occasion for this. For example, it is enough to have been in a particular radio cell, or to have been contacted by a particular person, at an inconvenient time, for a person to be exposed to wide-ranging investigations and to come under pressure to give explanations. In addition, the possibilities of abuse that are associated with such a collection of data aggravate its burdensome effect. This is particularly the case in view of the large number of varying private providers which store telecommunications data. Merely in view of the number of persons with duty of storage, the number of those who have and need to have access to such data is large. Since the duty of storage also affects small service providers, protection against abuse, notwithstanding all possible and necessary efforts of the legislature, has structural limits in view of the economic efficiency of those service providers. This is aggravated by the fact that the standards imposed on data management and the transmission of the data to the authorities require a high degree of technological competence and sophisticated software, and this inevitably entails the danger of weak points and the risk of manipulation by interested third parties. Particular weight also attaches to the storage of the telecommunications data because the storage itself and the intended use of the stored data are not directly noticed by the persons affected, but at the same time they include connections which are engaged in with an expectation of confidentiality. As a result of this, the storage of telecommunications traffic data without cause is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas.

213 b) Despite its extremely broad range and the weight of the encroachment associated with it, the legislature is not absolutely prohibited under constitutional law from introducing a six-month duty of storage, as provided for in § 113a TKG. However, under the established case-law of the Federal Constitutional Court, the state is strictly prohibited under constitutional law from creating a collection of personal data by way of precaution and retaining it for purposes that are indefinite or that cannot yet be determined (see BVerfGE 65, 1 (46); 100, 313 (360); 115, 320 (350); 118, 168 (187)). The precautionary storage without cause of telecommunications connections data is not in every case such a form of data

collection forbidden from the outset. Instead, if it is done for specific purposes, such a storage, as part of a statutory structure which is adequate to the encroachment (see V below), may also satisfy the requirements of proportionality in the narrow sense.

aa) The first relevant factor for this is that the storage of the telecommunications traffic data provided is realised not directly by the state, but by a duty imposed on the private service providers. In this way, the data are not yet combined at the time of storage itself, but remain distributed over many individual enterprises and are not directly available to the state in their entirety. In particular, the state has no direct access to the data; this must be ensured by appropriate legislation and technical precautions. The retrieval of the data by state agencies is done only in a second stage, and then related to a specific occurrence, in accordance with criteria to be legally defined in more detail. In this connection, the formulation of the provisions giving permission for retrieval and further use of the stored data may ensure that the storage is not made for purposes that are indefinite or cannot yet be determined. Thus, if such a duty of storage is imposed, it can and must be guaranteed that an actual taking notice and use of the data remains limited by well-defined provisions in a manner that takes account of the weight of the extensive collection of data and that restricts the retrieval and the actual use of the data to the part of the data pool that is absolutely necessary. At the same time, the separation of storage and retrieval structurally promotes the transparency and supervision – to be guaranteed in more detail by legislative drafting – of the use of the data. 214

bb) Nor does a six-month storage of the telecommunications traffic data in itself cancel the principle of Article 10.1 GG; it violates neither that Article's core of human dignity (Article 1.1 GG) nor its essence (Article 19.2 GG). Despite its extraordinary breadth, it remains effectively limited. Thus, for example, the contents of the telecommunications events are excluded from the storage, which is restricted to the traffic data. In addition, the duration of the storage is restricted. Admittedly, a period of six months' storage is very long, in view of the extent and informative value of the stored data, and it is at the upper limit of what can be justified from the point of view of proportionality. After the end of this period, however, citizens may rely on their data being deleted – unless they have exceptionally been retrieved for cause – and no longer being reconstructible by anyone. 215

cc) Nor does storage of the telecommunications traffic data for six months appear to be a measure directed towards total recording of the citizens' communications or activities as a whole. Instead, it takes up, in a manner still limited, the special significance of telecommunications in the modern world and reacts to the specific potential danger associated with this. The new means of telecommunications overcome time and space in a manner that is not comparable with other forms of communication, and that fundamentally excludes public awareness. In this way, at the same time, they facilitate concealed communications and actions of criminals and also enable scattered groups of only a few persons to form and to cooperate effectively. The communication, which is virtually without resistance, enables knowledge, readiness to act and criminal energy to be combined in a way that confronts warding off danger and criminal prosecution with novel tasks. Some criminal offences are committed directly with the help of the new technology. Integrated into a conglomeration of computers and computer networks which communicate with each other only through technology, such activities largely escape observation. At the same time, they can create new kinds of dangers, for example by attacks on third-party telecommunications. For effective criminal prosecution and warding off of danger, therefore, a reconstruction of telecommunications connections is of particular importance. 216

Another problem is that because telecommunications data are not publicly perceptible, there is also no social memory, unlike in other areas, which would permit past events to be reconstructed on the basis of chance memories. Telecommunications data are either deleted, after which they are completely lost, or stored, after which they are completely available. Consequently, in the decision as to how far such data are to be deleted or stored, the legislature may undertake a balancing of interests and take account of the concerns of state performance of duties. In this process, it may also include in its considerations the fact that the popularity of particular forms of contract used by telecommunications services providers (such as 217

the increase of flat-rate services) reduces the availability of such data where there is a strict duty of deletion of telecommunications traffic data which are not needed for the performance of the contract. In this respect too, the precautionary storage of telecommunications traffic data may be based on aspects which have a specific foundation in special features of modern telecommunications.

Conversely, the storage of the telecommunications traffic data may not be seen as a step in the direction of legislation aiming at as comprehensive as possible a storage by way of precaution of all data useful for criminal prosecution or the prevention of danger. Regardless of the structure of the provisions on use, such legislation would from the outset be incompatible with the constitution. For precautionary storage of telecommunications traffic data without cause to be constitutionally unobjectionable, this procedure must, instead, remain an exception to the rule. Nor may it, in interaction with other existing files, lead to virtually all activities of the citizens being reconstructible. It is therefore in particular essential for the justifiability of such storage that it is not made directly by state agencies, that it does not also contain the contents of the communications, and that commercial service providers are in principle prohibited from also storing details of the Internet sites visited by their customers. The introduction of the storage of telecommunications traffic data may therefore not serve as a model for the precautionary creation without cause of further data pools, but forces the legislature to exercise greater restraint in considering new duties or authorisations of storage with regard to the totality of the various data pools already in existence. It is part of the constitutional identity of the Federal Republic of Germany that the exercise of freedom of its citizens may not be totally be recorded and registered (on the constitutional identity retention principle, see BVerfG, judgment of the Second Senate of 30 June 2009 – 2 BvE 2/08 and others –, juris, marginal no. 240), and the Federal Republic of German must endeavour to preserve this in European and international contexts. Precautionary storage of telecommunications traffic data also considerably reduces the latitude for further data pools created without cause, including collections by way of European Union law. 218

dd) To summarise, a six-month storage of telecommunications traffic data to the extent provided by the legislature in § 113a.1 to 8 TKG is not disproportionate from the outset in the present circumstances. However, in order for it to be constitutionally unobjectionable, it is necessary for the formulation of the legislation on the storage and the use of the data to take appropriate account of the particular weight of such storage. 219

V.

The formulation of the legislation on a precautionary storage of telecommunications traffic data, as provided in § 113a TKG, is subject to specific constitutional requirements, in particular with regard to data security, to the extent of the use of the data, to transparency and to legal protection. Only if sufficiently sophisticated and well-defined provisions are drafted is the encroachment constituted by such storage proportionate in the narrow sense. 220

1. Storage of telecommunications traffic data in the extent of § 113a TKG requires the statutory guarantee of a particularly high standard of data security. 221

In view of the extent and the potential informative value of the retained data gathered by such storage, data security is of great importance for the proportionality of the challenged provisions. This applies in particular because the data are stored by private service providers which act under the conditions of profitability and cost pressure and in doing so have only limited incentives to guarantee data security. They act in principle in their private interest and are not bound by specific official duties. At the same time, the danger of illegal access to the data is great, for in view of their broad informative value, these data may be of interest to the most varied actors. A particular high standard of security is therefore necessary, which extends beyond the degree generally required under constitutional law for the storage of telecommunications data. Such requirements of data security here apply both to the storage of the data and to their transmission; similarly, effective safeguards are necessary to guarantee that the data are deleted. 222

In the statements in the oral hearing and in the written submissions to the present proceedings, experts referred to a broad spectrum of instruments to increase data security. For example, there was reference to separate storage of the data to be stored under § 113a TKG on computers which are also physically separate from each other and not connected to the Internet; an asymmetrical cryptographic encryption with keys stored separately; the requirement of the four-eyes principle for access to the data, combined with progressive methods of authentication for access to the keys; revision-proof recording of the access to the data and their deletion; and the use of automated error-correction and plausibility procedures. Supplementing such technologically oriented instruments, reference was also made to the creation of duties to provide information in the case of violations of data protection; the introduction of no-fault liability; or a strengthening of the claims to compensation for intangible damage, in order in this way to create an incentive to implement effective data protection. 223

The Basic Law does not lay down in detail what specific security measures are required. Ultimately, however, a standard must be guaranteed which, specifically taking into account the special features of the data pools created by precautionary storage of telecommunications traffic data, guarantees a particularly high degree of security. In this connection, it must be ensured that this standard – for example by recourse to legal concepts of non-constitutional law such as the state of the art (see Heibey, in: Roßnagel, *Handbuch Datenschutzrecht* , 2003, p. 575, marginal no. 19, p. 598, marginal no. 145; Tinnefeld/Ehrmann/Gerling, *Einführung in das Datenschutzrecht* , 4th ed. 2005, p. 628) – is oriented to the state of development of the discussion between specialists and constantly absorbs new knowledge and insights. It must therefore be provided that the enterprises with a duty of storage must adapt their measures to this in a verifiable manner, for example on the basis of security policies which are to be renewed periodically. By reason of the potential danger that follows from the data pools in question, it is not possible to subject the security requirements described to a free weighing of interests against general business considerations. If the legislature provides for comprehensive storage of telecommunications traffic data without exceptions, it is part of the necessary requirements that the providers affected can not only perform their duty of storage, but also comply with the corresponding data security requirements. Taking up the expert opinions, it is natural to conclude that in the present state of discussion, it is in principle necessary for the data to be stored separately, and for there to be sophisticated encryption, a secured access regime, using, for example, the four-eyes principle, and revision-proof recording, in order to adequately guarantee the security of the data under constitutional law. 224

There is a need for statutory provisions which lay down such a particularly high security standard in a qualified manner and are at all events fundamentally well-defined and legally binding. In this connection the legislature is free to entrust a regulatory agency with the technicalities of putting the prescribed standard into concrete terms. In this process, however, the legislature must ensure that the decision as to the nature and degree of the protective precautions to be taken does not ultimately lie without supervision in the hands of the respective telecommunications providers. The requirements to be made must either be laid down in sophisticated technical provisions – possibly graduated on various levels of legislation – or in a general manner and then be put in specific terms in a transparent manner by a binding individual decision of the regulatory authorities addressed to the individual enterprise. In addition, there is also a constitutional requirement of monitoring which is comprehensible to the public and which involves the independent data protection officer (see BVerfGE 65, 1 (46)) and a balanced system of sanctions which also attaches reasonable weight to violations of data security. 225

2. Storage of telecommunications traffic data as provided by § 113a TKG also requires statutory provisions on the use of these data. The drafting of these provisions on use, in a manner that is not disproportionate, thus not only decides on the constitutionality of these provisions, which in themselves constitute an encroachment, but also has an effect on the constitutionality of the storage as such. Under the case-law of the Federal Constitutional Court, the greater is the weight of the encroachment constituted by the storage, the more narrowly the requirements for the use of data and their extent must be defined in the relevant basic statutory provisions. The occasion, purpose and extent of the given encroachment and 226

the corresponding thresholds of encroachment must here be defined by the legislature in a manner that relates to a specific area and is precise and consists of well-defined provisions (see BVerfGE 100, 313 (359-360); 110, 33 (53); 113, 29 (51); 113, 348 (375); 115, 166 (191); 115, 320 (365); 118, 168 (186-187)).

227 The use of the data pools obtained from systematic storage without cause of virtually all telecommunications traffic data is therefore subject to particularly strict requirements. In particular, this use is not constitutionally permissible to the same extent as the use of telecommunications traffic data which the service providers are permitted to store under § 96 TKG, depending on the given operational and contractual circumstances, which can in part be influenced by the customers. In view of the systematic precautionary storage of traffic data for six months, which is unavoidable and complete and thus results in increased informative value, their retrieval is incomparably weightier. Since an analysis of these data permits conclusions that reach deep into private lives, and in certain circumstances makes it possible to make detailed personality profiles and track users' movements, it cannot automatically be assumed in this connection that recourse to these data carries fundamentally less weight than the content-based monitoring of telecommunications (on retrieval under the old law see BVerfGE 107, 299 (322)). Instead, the use of such data can also only be seen as proportionate if it serves particularly high-ranking reasons of public interest. A use of the data may therefore only be considered for overridingly important tasks of the protection of legal interests, that is, to punish criminal offences which threaten legal interests of paramount importance or to ward off dangers to such legal interests.

228 a) From this it follows for the prosecution of crimes that if the data are to be retrieved, there must at least be the suspicion of a serious criminal offence, based on specific facts. Together with the obligation to store data, the legislature must provide an exhaustive list of the criminal offences that are to apply here. In this, it has scope for assessment. It may either have recourse to existing lists or create its own list, for example in order to include criminal offences for which telecommunications traffic data are particularly important. However, if a criminal offence is to be categorised as serious, this must be objectively expressed in the statutory definition, in particular, for example, by the range of punishment provided (see BVerfGE 109, 279 (343 et seq., in particular 347-348). But a blanket clause or a mere reference to criminal offences of considerable significance is not sufficient.

229 In addition to laying down such a list of criminal offences in abstract terms, the legislature must ensure that recourse to the telecommunications traffic data stored by way of precaution is permissible only if the criminal offence prosecuted is also serious in the individual case (see BVerfGE 121, 1 (26) and the use of the data is proportionate; on criminal offences of considerable significance, see BVerfGE 107, 299 (322); on particularly serious criminal offences within the meaning of Article 13.3 GG, see BVerfGE 109, 279 (346)).

230 b) The use of the data in question must also be effectively restricted for the purpose of warding off danger. In this connection, permitting access to data with reference to lists of specific criminal offences which the use of the data is intended to prevent (see BVerfGE 122, 120 (142)) is not a suitable legislative approach. It removes the clarity from the requirements of the degree of endangerment to legal interests and leads to uncertainty where the definitions of legal offences penalise even acts preparatory to the commission of an offence and mere endangerments of legal interests. Instead, a solution might be for legislation to refer directly to the legal interests whose protection is to justify a use of the data, and to the degree of danger to these legal interests that must be attained as a threshold of encroachment. Such an approach corresponds to the character of warding off danger as the protection of legal interests and guarantees a direct connection to the main objective which is intended to justify the encroachment upon fundamental rights.

231 It follows from weighing the encroachment constituted by the storage and use of data and the importance of effective warding off of danger that retrieval of the telecommunications traffic data stored by way of precaution may only be permitted to ward off dangers to the life, limb or freedom of a person, to the existence or the security of the Federation or of a *Land* or to ward off a danger to public safety (see BVerfGE 122, 120 (141 et seq.)). In this connection, the enabling statute must at least require actual

evidence of a concrete danger to the legal interests to be protected. This requirement means that presumptions or general principles derived from experience are not sufficient to justify access to the data. On the contrary, specific facts must have been established which support the prognosis of a concrete danger. Here, the facts of the case must be such that there is sufficient probability in the individual case that specific persons will cause damage to the interests protected by the legislation in the foreseeable future, if the state does not intervene. The statements by the Senate in this connection on the requirements for online searches apply here with the necessary modifications (see BVerfGE 120, 274 (328-329)). The concrete danger is defined by three criteria: the individual case, the imminence of the time when a danger will become actual damage, and the relationship to individual persons who are likely to cause the damage. Admittedly, the retrieval of the data stored by way of precaution may already be justified at a time when it is not yet possible with sufficient probability to establish that the danger will arise in the near future, provided that particular facts indicate the threat of a danger to a legal interest of paramount importance. On the one hand, the facts must allow events to be identified, and it must at least be possible for the nature of these events to be put into concrete terms and for the time of their occurrence to be foreseeable, and on the other hand, the facts must indicate that particular persons will be involved, and at least enough must be known of their identity to allow the measure to be specifically targeted at them and concentrated on them. In contrast, insufficient account is taken of the weight of the encroachment upon fundamental rights if the actual occasion of the encroachment is located far in advance of a concrete danger to the interests protected by the legislation, and this concrete danger cannot yet be foreseen in concrete terms.

c) The constitutional requirements for the use of the data to ward off danger apply to all authorisations to encroach whose objective is preventive. They therefore also apply to the use of the data by the intelligence services. Since in all these cases the adverse effect of the encroachment is the same for those affected, there is no occasion to create different rules depending on the authority involved, for example to distinguish between police authorities and other authorities which have preventive duties, such as authorities for the protection of the constitution. The fact that police authorities and authorities for the protection of the constitution have difference duties and powers and may consequently undertake measures with different degrees of encroachment is in principle irrelevant to the weighting of a use of telecommunications traffic data stored by way of precaution comprehensively and for a long time (see BVerfGE 120, 274 (329-330)). Admittedly, differentiations between the authorisations of the various authorities with preventive duties may stand up to constitutional review (see BVerfGE 100, 313 (383); 120, 274 (330)). However, when the legislature provides for the individual powers of security authorities whose duty is advance intelligence, it is bound by the constitutional requirements which follow from the principle of proportionality (see BVerfGE 120, 274 (330-331)). In the present case, these lead to the conclusion that particular requirements must be imposed for the use of data both with regard of the legal interests to be protected and with regard to the threshold of encroachment to be observed in this connection. 232

There is no reason why these requirements should not apply to the intelligence services' performance of their tasks. Admittedly, the tasks of the intelligence services are fundamentally restricted to the collection of information to be supplied to the government. This reduces the weight of the encroachment in that the danger that the individual citizen is observed is not compounded by the danger of further measures following on this. At the same time, however, the weight needed to justify such encroachments is reduced, for mere information given to the government cannot prevent violations of legal interests. Preventing violations of legal interests is only possible as a result of subsequent measures taken by the authorities responsible for warding off danger, whose constitutional restrictions in the use of the data may not be circumvented by more extensive powers of use granted in advance. Apart from this, there is a particularly burdensome effect of such encroachments upon the citizens in that not only the given encroachment upon the secrecy of telecommunications as such is normally hidden, but virtually all the activities of the intelligence services are carried out in secret. The powers given to these services to use the 233

telecommunications traffic data which have been comprehensively stored by way of precaution thus particularly encourage the sense of being observed in a manner that cannot be monitored, and develop persistent intimidating effects on the exercise of freedom.

234 The Senate is aware that as a result of this, use by the intelligence services of the telecommunications traffic data stored by way of precaution will in many cases be impossible. However, this results from the nature of their tasks in advance intelligence and does not create a constitutionally acceptable occasion to relax the requirements for an encroachment of this kind that arise from the principle of proportionality (see BVerfGE 120, 274 (331)).

235 d) It must also be ensured that the restriction of the use of data to specific purposes also applies to the use of the data after they are retrieved and transmitted to the retrieving authorities, and there must be procedures in place to support this. In this respect it must be guaranteed by statute that after transmission the data are analysed without delay and, where they are irrelevant to the purposes of the collection, are deleted (see BVerfGE 100, 313 (387-388)). Apart from this, it must be provided that the data are destroyed as soon as they are no longer necessary for the purposes laid down, and that a record is made of this (see BVerfGE 100, 313 (362); 113, 29 (58)).

236 The telecommunications traffic data do not lose the protection given them by Article 10 GG as a result of the fact that a state authority has already obtained knowledge of them. The fundamental right's requirement that the use be clearly limited to specific purposes therefore also applies to the transmission of the data and information to further authorities. However, this does not exclude changes of purpose. But these require their own statutory basis, which in its turn must comply with constitutional requirements (see BVerfGE 100, 313 (360); 109, 279 (375-376)). In consequence, there may only be a provision for the transmitted telecommunications traffic data to be passed on to further agencies where as this is done to carry out duties for which direct access to these data would also be permissible (see BVerfGE 100, 313 (389-390); 109, 279 (375-76)); 110, 33 (73)). This must be recorded by the authority passing the data on (see BVerfGE 100, 313 (395-396)). Here, the limitation to specific purposes can be guaranteed only if it is still discernible after the collection that these are data which were stored without cause by way of precaution. Accordingly, the legislature must provide for an obligation to label these data (see BVerfGE 100, 313 (360-361)).

237 e) Finally, there may also be constitutional limits with regard to the extent of the data to be retrieved. Thus, for example, from the point of view of proportionality, many gradations can be identified within the various requests for information, for example depending on whether they relate only to one single telecommunications connection, whether they are directed at the transmission of data from one single radio cell at a particular time, whether they relate only to the communication between individual persons – possibly restricted to a particular period of time or a particular form of communication – and at the same time either include or exclude the location data, or whether they aim at a complete transmission of the data of a person to track that person's movements or create a personality profile of that person with as much detail as possible. With regard to the weight of the encroachment, it may also make a difference whether, when the data are transmitted, filters are used to screen out specific telecommunications connections to protect particular confidential relationships.

238 But in view of the high thresholds which under the above standards already apply fundamentally to the use of telecommunications traffic data stored by way of precaution, the legislature has legislative discretion when it provides in more detail for the scope of the use of data. In particular, the legislature is fundamentally also at liberty to leave such considerations of proportionality to the judge appointed to decide whether to order a retrieval of data, in the review of the individual case. As a product of the principle of proportionality, it is, however, constitutionally required that there should be a fundamental prohibition of transmission of data, at least for a narrowly defined group of telecommunications connections which rely on particular confidentiality. These might include, for example, connections to persons, authorities and organisations in the social or ecclesiastical fields which offer advice in situations

of emotional or social need, completely or predominantly by telephone, to callers who normally remain anonymous, where these organisations themselves or their staff are subject to other obligations of confidentiality in this respect (see § 99.2 TKG).

3. In addition, precautionary storage of telecommunications traffic data without cause and the use of these data are only proportionate if the legislature takes sufficient precautions to ensure the transparency of the use of data and to guarantee effective legal protection and effective sanctions. 239

a) The requirements of the constitutionally unobjectionable use of data obtained by such storage include requirements as to transparency. As far as possible, the use of the data must be open. Failing this, it is in principle necessary for the persons affected to be informed, at least subsequently. If, exceptionally, even this subsequent notification is not made, there must be a judicial decision with regard to the non-notification. 240

aa) Precautionary storage without cause of all telecommunications traffic data for a period of six months is such a serious encroachment *inter alia* because it can create a sense of being permanently monitored; in an unforeseen manner, it permits a high degree of knowledge of private life, without the recourse to the data being directly perceptible by or visible to the citizen. The individual does not know which state authority knows what about him or her, but knows that the authorities may know a great deal about him or her, including highly personal matters. 241

By effective provisions on transparency, the legislature must counteract the diffuse sense of threat which may attach to data storage as a result of this. Provisions on information for the persons affected by the collection or use of data are generally among the elementary instruments of constitutional data privacy (see BVerfGE 100, 313 (361); 109, 279 (363-364)); 118, 168 (207-208)); 120, 351 (361-361)). In this respect, strict requirements must be imposed on the use of the data pools resulting from precautionary storage of telecommunications traffic data without cause, which are extensive and offer a variety of information. On the one hand, these requirements must reduce a sense of threat, which arises from ignorance as to the factual relevance of the data, must counteract speculations which create a sense of insecurity, and must make it possible for those affected to address such measures in public discourse. On the other hand, such requirements may also be derived from the precept of effective legal protection under Article 10.1 GG in conjunction with Article 19.4 GG. Without knowledge, those affected may assert neither unlawful official use of the data nor any rights to deletion, correction or legal redress (see BVerfGE 100, 313 (361); 109, 279 (363); 118, 168 (207-208)); 120, 351 (361)). 242

bb) The requirements for transparency include the principle that the collection and use of personal data should be open. Use of the data without the knowledge of the person affected is constitutional only if otherwise the purpose of the investigation served by the retrieval of data would be frustrated. The legislature may in principle assume that this is the case for warding off danger and carrying out the duties of the intelligence services. In contrast, in criminal prosecution there is also the possibility that data may be collected and used openly (see § 33.3 and 33.4 StPO). In this connection, investigation measures are sometimes also taken in other matters with the knowledge of and in the presence of the suspect (see for example §§ 102, 103, 106 StPO). Accordingly, persons affected must as a general rule be notified before the retrieval or transmission of their data. There may only be a provision for secret use of the data here if such use is necessary and is ordered by a judge in the individual case. 243

Insofar as the use of the data is secret, the legislature must provide for a duty of information, at least subsequently. This must guarantee that the persons to whom a request for data retrieval directly applied – whether as suspects, as persons endangering public security, or as third parties – are in principle informed, at least subsequently. The legislature may provide for exceptions in weighing the notification against constitutionally protected legal interests of third parties. However, these must be restricted to what is absolutely necessary (see BVerfGE 109, 279 (364)). It is conceivable that there may be exceptions to the duties of notification in connection with the prosecution of criminal offences, for example where knowledge of the encroachment upon the secrecy of telecommunications would result in it failing to 244

achieve its objective, if the notification cannot be made without endangering the life and limb of a person or if the concerns of an affected person which carry more weight conflict with it, for example because the notification of a measure that has had no further consequences would increase the encroachment upon fundamental rights (see BVerfGE 100, 313 (361); 109, 279 (364 et seq.)). If there are compelling reasons which also exclude subsequent notification, this must be judicially confirmed and reviewed at regular intervals (see BVerfGE 109, 279 (367-368)). In a corresponding manner, it is also necessary to structure the duties of notification with regard to the use of the data for purposes of warding off dangers or of intelligence service duties.

In contrast, it is not constitutionally required to provide for comparably strict notification duties for persons whose telecommunications traffic data were only by chance collected together with others and who are not themselves the target of the actions of the authority. There may be a large number of such persons involved in the analysis of telecommunications traffic data, but knowledge of their data for a short period of time may not leave traces or have consequences for the persons involved. On the contrary, in an individual case a notification may aggravate the encroachment upon their fundamental rights (see BVerfGE 109, 279 (365); Chamber Decisions of the Federal Constitutional Court (*Kammerentscheidungen des Bundesverfassungsgerichts* – BVerfGK) 9, 62 (81)). In these cases, it is in principle possible for a notification to be withheld even if the persons involved were affected by the measure, but only trivially, and it is to be assumed that they have no interest in the notification. There is no need for judicial confirmation of this decision on the weighing of interests. 245

b) In addition, the proportionate formulation of precautionary storage of telecommunications traffic data and of their use requires that effective legal protection and adequate sanctions are guaranteed. 246

aa) In order to guarantee effective legal protection, a retrieval or transmission of these data must fundamentally be made subject to judicial authority. 247

Under the case-law of the Federal Constitutional Court, in the case of investigation measures which create a serious encroachment upon fundamental rights preemptive supervision by an independent instance may be constitutionally required. This applies in particular if the encroachment upon fundamental rights is made secretly and is not directly perceptible by the person affected (see BVerfGE 120, 274 (331)). This may be the case with regard to the retrieval and transmission of telecommunications traffic data. In view of the weight of the encroachment constituted by this, the discretion of the legislature is reduced insofar as such measures must fundamentally be subjected to judicial authority. Because they are independent from a personal and factual point of view and because they are bound solely by the law, judges can best and most reliably protect the rights of the person affected in the individual case (see BVerfGE 77, 1 (51); 103, 142 (151); 120, 274 (332)). Under Article 10.2 sentence 2 GG, there is an exception for the supervision of encroachments upon the freedom of telecommunications by the intelligence services. Here, a preemptive judicial supervision may be replaced by supervision – equally relating specifically to the measure in question – by an agency or auxiliary agency appointed by parliament (see BVerfGE 30, 1 (21)). 248

The legislature must make provisions defining the requirement of preemptive judicial review in a concrete form with well-defined provisions, and must combine this with strict requirements as to the contents and the grounds on the judicial order (see BVerfGE 109, 279 (358-359)). At the same time, it follows from this that there must be a sufficiently substantiated justification and restriction of the retrieval of the data requested; it is only this that enables the court to exercise effective supervision (see BVerfGE 103, 142 (160-161)). It is only on this basis that the court making the order can and must on its own responsibility form an assessment as to whether the use of the data applied for complies with the statutory requirements. Part of this is a careful review of the requirements of the encroachment, including in particular the threshold of encroachment laid down by statute. The court must justify its order with substantial detail. In addition, the data to be transmitted, in compliance with the principle of proportionality, 249

must be defined sufficiently selectively and clearly (see BVerfGE 103, 142 (151)), in order that the service providers do not have to undertake their own examination of the matter. These service providers may be required and permitted to transmit data only on the basis of clear orders on data transmission.

The effectiveness of the supervision also requires that the data, on the basis of the order, must be 250
filtered out by the telecommunications enterprises as third parties with a duty of storage, that is, that the authorities are not given direct access to the data. In this way, the use of the data is referred to the cooperation of a number of actors and thus to decision-making structures which mutually supervise each other.

bb) It is also constitutionally required that a legal protection procedure is available to subsequently 251
review the use of the data. Where persons affected had no opportunity before the measure was carried out to defend themselves against the use of their telecommunications traffic data, they must be given the possibility of subsequent judicial review.

cc) Finally, a legislative formulation that is not disproportionate also requires effective sanctions for 252
violations of rights. If even serious breaches of the secrecy of telecommunications were ultimately to remain without sanction, with the result that the protection of the right of personality, even in its specific manifestation in Article 10.1 GG, atrophied in view of the intangible nature of this right (see BVerfG, order of the First Chamber of the First Senate of 11 November 2009 – 1 BvR 2853/08 –, juris, marginal no. 21; BGHZ 128, 1 (15)), this would contradict the duty of the state to enable individuals to develop their personality (see BVerfGE 35, 202 (220-221); 63, 131 (142-43)); 96, 56 (64)) and to protect them against third-party threats to the right of personality (see BVerfGE 73, 118 (210); 97, 125 (146); 99, 185 (194-195)); BVerfGK 6, 144 (146)). This might in particular be the case if data obtained without authorisation were permitted to be used without hindrance, or an unauthorised use of the data were routinely to remain without compensation to satisfy the persons affected, for lack of tangible damage.

However, in this connection the legislature has a wide legislative discretion. Here, it can in particular 253
consider how far corresponding provisions might be incorporated into the general structure of the law of criminal procedure or into current liability law. In this respect it may also take account of the fact that in the case of serious violations of the right of personality, the current law may already provide both for prohibitions of use on the basis of a weighing of interests (see BVerfGE 34, 238 (248 et seq.); 80, 367 (375-376)); 113, 29 (61); BVerfGK 9, 174 (196); Decisions of the Federal Court of Justice in Criminal Matters – *Entscheidungen des Bundesgerichtshofes in Strafsachen* (BGHSt) 34, 397 (401); 52, 110 (116)) and for liability for intangible damage (see BVerfGE 34, 269 (282, 285-286); BVerfGK 6, 144 (146-147); BVerfG, order of the First Chamber of the First Senate of 11 November 2009 – 1 BvR 2853/08 –, juris, marginal no. 21; Decisions of the Federal Court of Justice in Civil Matters – *Entscheidungen des Bundesgerichtshofes in Zivilsachen* (BGHZ) 128, 1 (12)). For the decision as to whether more extensive provisions are needed in this connection, the legislature is not prevented by this from initially considering whether case-law on the basis of applicable law possibly takes sufficient account in the constitutionally required manner of the particular severity of the violation of personality which the unauthorised acquisition or use of the data in question here usually constitutes.

4. Less stringent constitutional standards apply to a use of the data stored by way of precaution which is 254
only indirect, in the form of official rights to information from the service providers with regard to the owners of particular IP addresses which the service providers are to identify by use of the stored data. The creation of such rights to information is permissible, independent of restrictive lists of legal interests or criminal offences, to a greater extent than the retrieval and use of the telecommunications traffic data themselves.

a) When information on the owners of particular IP addresses can only be determined by resorting to 255
telecommunications traffic data stored by way of precaution, it is not constitutionally necessary to satisfy the particularly stringent requirements which otherwise apply to the use of such data.

It is important on the one hand for this purpose that the authorities do not themselves acquire any knowledge of the data to be stored by way of precaution. In connection with such rights of information, the authorities do not themselves retrieve the data that have been stored by way of precaution without cause, but are merely given personal information as to the owner of a particular connection, who is determined by the service providers by recourse to these data. In this connection, the informative value of these data is strictly limited. The use of the data stored by way of precaution only provides the information as to what owner was registered on the Internet with regard to an IP address that is already known, for example where the address has been determined by other investigations. The formal structure of such information is similar in certain respects to the retrieval of the name of the owner of a telephone number. Its informational value is limited in range. It is not possible to carry out systematic investigation over a long period of time or to prepare personality profiles and track people's movements on the basis of such information alone. 256

It is also crucial that for such information only a small section of the data, which is determined in advance, is used; the storage of these particular data in itself could therefore be ordered subject to far less strict requirements. If solely the Internet access data necessary for such information were stored in order to identify dynamic IP addresses, this would be considerably less burdensome than the virtually complete storage of the data of all telecommunications connections. It follows from considering the combination of these aspects that the requirements which otherwise apply to telecommunications traffic data stored for use by way of precaution do not apply in the same way to such information. 257

b) However, creating official rights to information in order to identify IP addresses is also of substantial weight. In doing this, the legislature influences the conditions of communication in the Internet and limits its anonymity. On this basis, in conjunction with the systematic storage of Internet access data, it is possible to a great extent to establish the identity of Internet users. Where private persons who find that they are injured on the Internet register the relevant IP address and make a criminal complaint, or where the authority itself traces IP addresses, these addresses can be connected to specific owners, and the communication processes of this IP address can be attributed to individuals with substantial probability. 258

But despite a certain similarity, attributing an IP address to the owner of a connection cannot be equated to the identification of a telephone number with regard to its weight for the person affected. Telephone numbers are permanent identifiers, which are exchanged between the users, and therefore it is possible to retrieve the details of their owners even independently of specific telecommunications acts. In contrast, information on the owner of a dynamic IP address necessarily also contains the information that this IP address was used at a particular time, and from what connection it was used. In addition, the telephone number may easily be concealed from private persons, whereas the IP address can basically be concealed only by the use of anonymisation services. The potential relevance to the right of personality of a retrieval of the identity of the owner of an IP address is also different from that of the owner of a telephone number. On the mere basis of the large number of new connections which are made in each case by visiting Internet sites, it has more informative value than a retrieval of telephone numbers. The knowledge that contact to an Internet site has been established also has a different substantive meaning: since the contents of Internet sites, unlike the spoken word in telephone conversations, are electronically fixed and can be retrieved again for a long period, they may often reliably be used to reconstruct the subject with which the communicating person was dealing. The connecting of the IP address to an individual as that person's "Internet telephone number" thus at the same time gives information on the contents of the communication. The distinction between external connection data and contents of a conversation, which applies to a telephone call, is broken down here. If a visitor to a specific Internet site is identified by information via an IP address, not only is it known with whom the visitor had contact, but normally also what were the contents of the contact. 259

Conversely, admittedly, there is also increased interest in the possibility of being able to attribute communication connections in the Internet to the relevant actors, in order to protect legal interests or to safeguard the legal order. In view of the increasing importance of the Internet for the most varied areas 260

and events of everyday life, the danger increases that it will be used for criminal offences and violations of rights of many kinds. In a state under the rule of law, even the Internet may not be a legal vacuum. It is therefore a legitimate concern for the legislature, where relatively serious violations of rights occur, to be able to relate Internet contacts to individuals. To the extent that telecommunications traffic data must be analysed by the service providers in order to give such information in the current technological conditions, in which IP addresses are predominantly allocated only for an individual session ("dynamically"), this therefore encounters no fundamental objections. In addition, in order to guarantee reliable attribution of these addresses for a certain period of time, the legislature may provide for the relevant data to be retained or for comprehensive recourse to be permitted to data retained in this way by the service providers. In this connection, the legislature has legislative discretion.

c) Accordingly, the legislature may permit such information, even independently of restrictive lists of legal interests or criminal offences, for the prosecution of criminal offences, for warding off danger and for the intelligence services to carry out their duties, on the basis of general authorisations to encroach provided by specific branches of law. (see Bock, in: Geppert/Piepenbrock/Schütz/Schuster, *Beck'scher Kommentar zum TKG* , 3rd ed. 2006, *§ 113* , marginal no. 7; Graulich, in: Arndt/Fetzer/Scherer, *TKG* , 2008, *§ 113* , marginal no. 8). Admittedly, with regard to the thresholds of encroachment, it must be ensured that information may not be obtained at random, but only on the basis of a sufficient initial suspicion or of a concrete danger on the basis of facts relating to the individual case. In this connection, the requirement of a concrete danger based on factual evidence applies to the intelligence services just as to all authorities competent to ward off danger to public security and order. The legal and factual basis of such requests for information must be placed on the record. For information of this kind, however, it is not necessary to provide for a requirement of judicial authority. 261

But the substantial weight of the encroachment made by such information does not permit it to be made available generally and without restrictions to prosecute or prevent every regulatory offence whatsoever. For anonymity in the Internet to be lifted, there must at least be an adverse effect on a legal interest, and the legal system must accord particular significance to this adverse effect in other contexts too. This does not completely exclude such information being given to prosecute or prevent regulatory offences. But they must be regulatory offences that are particularly serious – even in the individual case – and they must be expressly named by the legislature. 262

Nor is there any reason to revoke the principle of transparency (see C V 3 above) for the identification of IP addresses. The person affected, who may as a rule assume that he or she is using the Internet anonymously, has, in principle, the right to learn that this anonymity has been removed, and why. Accordingly, the legislature must at all events provide for duties of notification, insofar as and as soon as this does not frustrate the purpose of the information or other predominant interests of third parties or of the persons affected themselves do not conflict with this. Where, in exceptional cases, in accordance with statutory provisions to this effect, there is no notification, the reason for this must be put on record. However, in this case there is no need for judicial confirmation of the failure to notify. 263

5. The constitutionally required guarantee of data security and of a restriction of the use of data, in well-defined Federal provisions, which satisfies the requirements of proportionality, is an inseparable element of legislation creating a duty of data storage, and it is therefore the responsibility of the Federal legislature, which imposes the duty. In contrast, the responsibility for creating the retrieval provisions themselves and for drafting the provisions on transparency and legal protection depends on the legislative competence for the respective subject-matter. 264

a) Under Article 73.1 no. 7 GG, where questions of data security need to be decided in connection with the duty of the service providers to store telecommunications traffic data by way of precaution without cause, this, as an immediate component of the duty of storage and of the consequences legally associated with this, is the responsibility of the Federation. This includes not only the provisions on the security of the stored data, but also the provisions on the security of the transmission of the data, and in this connection the guarantee of protection of confidential relationships (see above C V 1 and C V 2 e). 265

In addition, the Federation must also ensure that there is a sufficiently precise restriction of the purposes of data use served by the storage which satisfies constitutional requirements. The reason for this lies in the indissoluble constitutional connection between data storage and purpose, as is held in established case-law of the Federal Constitutional Court: Data may from the outset be stored only for particular purposes, relating to a specific area, in precise and well-defined provisions, and it is therefore sufficiently guaranteed at the time of storage that the data will be used only for such purposes as justify the weight of the storage. There can be no abstract justification of storage in itself; it can be justified only where it serves sufficiently important and concretely named purposes (see BVerfGE 65, 1 (46); 118, 168 (187-188)). In contrast, it is not permissible to create a data pool in advance, independent of such purposes, whose use is left to later decisions of various state instances, depending on their requirements and political discretion. In such a case, the constitutionality of the storage could not yet be assessed, for lack of sufficiently foreseeable and restricted purposes, at the date of the encroachment constituted by the storage. In addition, its scope would be neither foreseeable to citizens nor restricted in accordance with the principle of proportionality. In the interaction of the Federation and the *Länder* too, this substantive connection between storage and purpose of use of the data as the crucial link between encroachment and justification may not be severed. The competence to guarantee this link accrues to the Federation under Article 73.1 no. 7 GG by virtue of factual connection (see above C III 2). 266

The provisions to be made by the Federation in this regard in connection with the storage include drafting the qualified requirements for use of the data for the purpose of criminal prosecution, warding off of danger or preventing danger by the intelligence services under the conditions developed above. They also include the necessary provisions to ensure that the further use of the data remains limited to specific purposes, in particular in the form of duties of labelling and recording. 267

b) In contrast, when the Federation passes provisions on the duty of storage, it does not automatically also have the responsibility as to whether and to what extent the data may be resorted to in connection with the purposes to be provided by the Federation. The passing of provisions governing the retrieval of data itself is no longer fundamentally the responsibility of the Federation, but follows the general rules on legislative competence. According to these, the authorisation to retrieve the data cannot be based on Article 73.1 no. 7 GG, but is to be granted in each case on the basis of the rule on jurisdiction which governs the legislation on the tasks for which the data is to be used (see BVerfGE 113, 348 (368); 114, 371 (385)). In the area of warding off danger and of the duties of the intelligence services, the responsibility is thus largely with the *Länder* . The constitutionally required restriction of the purposes of use must be provided for concurrently with the storage, by reason of the link between encroachment and justification under data protection law; unlike this, not only the authorisation of retrieval, but also the further constitutional requirements of the formulation of the data use, such as in particular the provisions on the notification of the persons affected and the guarantee of effective legal protection, can and must be left to later acts of legislation of the *Länder* . In this connection, the *Länder* themselves bear direct responsibility for the constitutionality of these provisions. 268

VI.

The challenged provisions do not satisfy these requirements. Admittedly, the reason why § 113a TKG conflicts with the fundamental right to protection of the secrecy of telecommunications under Article 10.1 GG is not simply that the scope of the duty of storage under §§ 113a.1 to 113a.7, 11 TKG would have to be considered disproportionate from the outset. But the provisions on data security, on the purposes and the transparency of the use of data and on legal protection do not satisfy the constitutional requirements. In consequence, the whole legislation lacks a structure complying with the principle of proportionality. §§ 113a, 113b TKG and § 100g StPO, insofar as the latter permits the retrieval of the data to be stored under § 113a TKG, are therefore incompatible with Article 10.1 GG. 269

1. § 113a TKG is not unconstitutional merely because of its scope. The legislature may deem the duty of storage created by § 113a TKG, which under § 113a.1 to § 113a.7 extends without cause to virtually all traffic data of publicly accessible telecommunications services, to be suitable, necessary and proportionate in the narrow sense to increase the effectiveness of criminal prosecution and the prevention of danger (see above C IV). Despite its scope, the provision is still sufficiently restricted with regard to the extent of the data covered. As § 113.8 TKG expressly states, the contents of telephone conversations, faxes and emails may not be stored, nor may the websites or service providers which a user has contacted on the Internet. In addition, in § 113a.1, 11 TKG the legislature has provided for a period of storage which is still constitutionally acceptable, given a duration of six months and a period of one month for deletion immediately following this. Similarly, at the present time it cannot be determined that the provision, in combination with other provisions, aims at or results in the creation of a general comprehensive data pool for the greatest possible reconstruction of all activities whatsoever of the citizens. In this connection, importance attaches to the application of the principle of data economy, which in other respects pervades data protection law, and to a large number of duties of deletion, with which the legislature fundamentally endeavours to prevent the creation of avoidable data pools. In this connection, the relevant factors for this assessment are in particular, for example, §§ 11 et seq. of the Telemedia Act (*Telemediengesetz* – TMG), which fundamentally subject services providers under the Telemedia Act to an obligation to delete data which are not necessary for the statement of costs (see § 13.4 no. 2, § 15 TMG) and in this way, against private-sector incentives too prevent the contents of the use of the Internet from being recorded in general commercial data pools and thus remaining reconstructible. § 113a TKG can therefore not be understood as the expression of a general public provision of data for the future for purposes of criminal prosecution and prevention of danger, but despite its breadth remains a limited exception which attempts to take account of the particular challenges of modern telecommunications for criminal prosecution and prevention of danger. 270

2. In contrast, the guarantee of a particularly high standard of security, which is constitutionally necessary for such a data pool, is missing. In this respect, § 113a.10 TKG only provides the duty, which remains undefined, to ensure by technical and organisational measures that access to the stored data is possible solely for persons who are specially authorised, and apart from this refers only to the care which is necessary in general in the area of telecommunications. There is therefore no provision which takes account of the particularly strict standards required of the security of the extensive and informative data pool under § 113a TKG. §§ 88 and 109 TKG, which are referred to with regard to their contents, do not guarantee such a particularly high security standard, but permit a wide range of relative degrees, corresponding to their wide area of application. This applies in particular to § 109 TKG. Thus, for example, under § 109.1 TKG every service provider must take appropriate technical precautions or other measures to protect the secrecy of telecommunications and the telecommunications and data processing systems against unauthorised access. In this connection, in order to determine the appropriateness, § 109.2 sentence 4 TKG is referred to (see Klesczewski, in: Säcker, *Berliner Kommentar zum TKG* , 2nd ed. 2009, *§ 109* , marginal no. 12). This provides that the measures are appropriate if the technical effort and economic expense are in an appropriate proportion to the importance of the rights to be protected. Taking as a basis the standards developed above, these do not sufficiently guarantee the specific requirements of the protection of the data stored under § 113a TKG. The standard laid down by statute of “appropriate technical precautions or other measures” merely requires that “account should be taken” of the state of technological development (see § 109.2 sentence 2 TKG; Klesczewski, in: Säcker, *Berliner Kommentar zum TKG* , 2nd ed. 2009, *§ 109* , marginal no. 13), and in doing so qualifies the security requirements in a way that remains undefined by introducing general considerations of economic adequacy in the individual case. In addition, putting this standard in more specific terms is left to the individual telecommunications service providers, which in turn have to offer their services subject to the conditions of competition and cost pressure. 271

Nor is it ensured by statutory orders or by orders of the regulatory authorities that these standards are put into specific terms. In particular, § 110 TKG does not guarantee that adequate security standards apply. Admittedly, the delegated legislation to be passed under this statute (see § 110.2 and 3 TKG) may include aspects of data security. However, this statute – which is primarily determined by technical objectives – neither contains substantive standards, nor does it otherwise take up the aspect of data security. Apart from this, even two years after the duty of storage of § 113a TKG entered into force, the Telecommunications Interception Order (*Telekommunikationsüberwachungsverordnung* – TKÜV) has not been adapted to take account of the reform of the law. Correspondingly, under § 110.3 TKG, the Technical Guideline for the Implementation of Statutory Measures to Monitor Telecommunications and for Requests for Information for Traffic Data (*technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten* – TR-TKÜV) – published in December 2009 under § 110.3 sentence 3 TKG on the website of the Federal Network Agency (see Federal Network Agency, Amtsblatt 2009, p. 4706) – will come into effect only one year after this adaptation (see Inhaltsangabe 1 (Regelungsbereich) TR-TKÜV; Teil B 1 (Grundsätzliches) TR-TKÜV). 272

Nor does § 109.3 TKG guarantee sufficient data security. Admittedly, the statute provides that operators of telecommunications equipment must appoint security officers and prepare a security policy, which must be submitted to the Federal Network Agency. In addition, the policy must be adjusted and resubmitted later if the “circumstances” on which it is based are changed. However, this does not reliably guarantee a particular high security standard. Thus, for example, the provision only applies to equipment operators, but not to all the persons targeted by § 113a TKG, which also applies to other service providers. In addition, § 109.3 TKG refers substantively only to the insufficient requirements of § 109.1 and 109.2 TKG. Nor is a continuing and verifiable adaptation of the security standard to the state of the art in technology guaranteed by well-defined provisions. In this connection, it is not clear whether § 109.3 sentence 4 TKG also requires an adaptation to the technological development of protective measures and to developing legal security standards. At all events, there is no obligation for a periodical updating of the security policy which could enable effective supervision in this respect. 273

Nor can § 9 of the Federal Data Protection Act (*Bundesdatenschutzgesetz* – BDSG) in conjunction with the relevant schedule compensate for the absence of adequate security standards in the Telecommunications Act. Notwithstanding its high standards, some of which are abstract, this provision, which in any case may only be applied in the alternative (see Fetzer, in: Arndt/Fetzer/Scherer, *TKG* , 2008, before § 91, marginal no. 10; Klesczewski, in: Säcker, *Berliner Kommentar zum TKG* , 2nd ed. 2009, § 91 marginal no. 15), is too general to ensure in a sufficiently specific and reliable manner the particularly high security standards with regard to the data to be stored under § 113a TKG. 274

All in all, therefore, there is no guarantee in a binding form and in well-defined provisions of a particularly high security standard for the data to be stored under § 113a TKG. Neither are the instruments cited by the experts in the present proceedings as central elements (separate storage, asymmetric encryption, the four-eyes principle in conjunction with advanced authentication procedures for access to the keys, revision-proof recording of access and deletion) imposed on the persons with a duty of storage in an enforceable manner, nor are other precautions which guarantee a comparable level of security imposed on them. Nor is there a balanced system of sanctions that attributes no less weight to violations of data security than to violations of the duties of storage themselves. The range of administrative fines for non-compliance with the duties of storage is markedly broader than that for the violation of data security (see § 149.2 sentence 1 in conjunction with § 149.1 nos. 36 and 38 TKG). The current legal situation therefore does not satisfy the constitutional requirements of the security of a data pool as is created by § 113a TKG. 275

3. The provisions on transmission and use of the data under § 113b sentence 1 half-sentence 1 TKG do not satisfy the constitutional requirements. 276

a) Firstly, the provisions on the use of the data for criminal prosecution are incompatible with the standards developed from the principle of proportionality. 277

aa) § 113b sentence 1 no. 1 TKG in conjunction with § 100g StPO does not satisfy the particularly stringent requirements which must be satisfied for access to the data stored under § 113a TKG to be permitted. Admittedly, in these provisions the legislature has laid down a sophisticated objective of data use for criminal prosecution which is also, pursuant to Article 74.1 no. 1 and Article 72.1, final. Here, however, the legislature permits similar standards to apply for the use of the data as have applied until now for the collection of telecommunications traffic data which the service providers were entitled to store under § 96 TKG depending on their operational and contractual requirements to a more limited extent and in such a way that the individual could in part contract out of this. This does not take sufficient account of the particularly serious encroachment constituted by the systematic precautionary data storage without cause of § 113a TKG. 278

Even § 100g.1 sentence 1 no. 1 StPO does not ensure that in general and also in the individual case only serious criminal offences may be the occasion for collecting the relevant data, but – independently of an exhaustive list – merely generally accepts criminal offences of substantial weight as sufficient. § 100g.1 sentence 1 no. 2, sentence 2 StPO satisfies the constitutional standards even less, in that it accepts every criminal offence committed by means of telecommunications, regardless of its seriousness, as the possible trigger for data retrieval, depending on a general assessment in the course of a review of proportionality. This provision makes the data stored under § 113a TKG usable with regard to virtually all criminal offences. As a result, in view of the increasing importance of telecommunications in everyday life, the use of these data loses its exceptional character. Here, the legislature no longer confines itself to the use of data to prosecute serious criminal offences, but goes far beyond this, and thus also beyond the objective of data storage specified by EU law, which also in turn is restricted to the prosecution of serious criminal offences, without including the prevention of danger. Admittedly, a use of these data can be very useful, especially for the prosecution of criminal offences committed by means of telecommunications, and therefore restricting it may in some cases make their successful investigation more difficult or even impossible. However, it is in the nature of the guarantee of Article 10.1 GG and of the proportionality standards associated with this that not every measure that is useful, and in the individual case may also be necessary, for criminal prosecution is constitutionally permissible. Conversely, as a consequence of the standards that are decisive here, telecommunications do not in their entirety become a legal vacuum, even in the area of less serious criminal offences: the legislature may provide that information under § 113.1 TKG – including information indirectly using the data stored under § 113a TKG – is available for the investigation of all criminal offences (see above C V 4 c). Similarly, as a result of this, recourse under § 100g StPO to telecommunications traffic data stored otherwise than under § 113a TKG remains possible. 279

bb) In addition, § 100g StPO fails to comply with the constitutional requirements in that it fundamentally permits retrieval of data even without the knowledge of the person affected (§ 100g.1 sentence 1 StPO). The constitutional requirements of the transparency of use of data only permit the data stored under § 113a TKG to be collected secretly if this is necessary for reasons carrying more weight which must be more precisely defined by statute, and if it is judicially ordered. 280

cc) Nor does the formulation of the duty of notification in every respect comply with the standards developed above. However, the extent of the duties of notification provided for is not as such open to any constitutional objections. §§ 101.1, 101.4 and 101.5 StPO, in conformity with the case-law of the Federal Constitutional Court (see BVerfGE 109, 279 (363 et seq.)), provides for complex provisions which balance the principle of subsequent notification of the person affected, in a manner which is constitutionally workable, with predominant concerns which exceptionally arise in the individual case. Another aspect which is unobjectionable in this context is the fact that under § 101.4 sentence 4 StPO, persons affected to whom the retrieval of data did not apply are not to be notified in every case, but only in accordance with a weighing of interests. In this weighing of interests, the interests of persons indirectly affected can and must be taken sufficiently into account. 281

In contrast, the provisions on judicial review for cases in which a notification may be omitted are inadequate. § 101.6 StPO provides for judicial review only when notification is deferred under § 101.5 StPO, but not when there is no notification, under § 101.4 StPO. This does not take sufficient account of the high value of the notification for transparent use of the data stored under § 113a TKG. Where data retrieval relates directly to traffic data of a specific person, that person absolutely must be subsequently notified unless there is a judicial review of the relevant grounds for an exception. Such a judicial review is missing in the cases in which there is to be no notification under § 101.4 sentence 3 StPO by reason of predominant concerns of a person affected. 282

dd) In contrast, the judicial review of data retrieval and data use is itself guaranteed in a manner that complies with constitutional requirements. Under § 100g.2 sentence 1, § 100b.1 sentence 1 StPO, the collection of the data stored under § 113a TKG requires a judicial order. Nor does the judicial order authorise the authorities to have direct access to the data; instead, it obliges the service providers to filter them out and transmit them, in a separate intermediate process in compliance with the order. In addition, under § 101.1, 101.7 sentences 2 to 4 StPO there is the possibility subsequently to arrange a judicial review of the lawfulness of the measure. It is not apparent that these provisions do not, as a whole, guarantee effective legal protection. 283

However, the statutory provisions on the formal requirements of the judicial order are not formulated in sufficiently well-defined provisions. § 100g.2 in conjunction with § 100b.2 StPO merely lays down the minimum requirements of the operative part of the order; apart from this, the general obligation to give reasons for a decision applies to decisions under § 34 StPO. In revising the legislation, the legislature should consider whether it would be appropriate to emphasise the strict requirements of a substantiated justification of judicial orders (see BVerfGE 103, 142 (151); 107, 299 (325); 109, 279 (358-359)) by way of a special and tailor-made provision. At all events, it must be ensured by statute that the extent of the data to be transmitted is described in the judicial order sufficiently selectively and unambiguously for the service providers, in a manner that satisfies the principle of proportionality. 284

b) The challenged provisions also fail to satisfy the constitutional requirements with regard to the retrieval and use of the data stored under § 113a TKG for warding off danger and for the tasks of the intelligence services. The very structure of § 113b sentence 1 nos. 2 and 3 TKG does not satisfy the requirements of sufficient limitation of the purposes of use. In this provision, the Federal legislature contents itself with sketching in a merely general manner the fields of duty for which data retrieval is to be possible, without stating the purposes of use in concrete terms. Instead, it leaves the purposes of use to be defined in concrete terms by later legislation, including in particular *Länder* legislation. In this way the Federal legislature does not satisfy its responsibility for the constitutionally required limitation of the purposes of use. If it orders that telecommunications traffic data are to be stored, it is at the same time obliged to lay down additionally in a binding form the purposes of use and thresholds of encroachment that are necessary to constitutionally justify the storage, and to bindingly lay down the consequential provisions that are necessary to guarantee that the use is limited to specific purposes. § 113b half-sentence 1 TKG contains no such provisions. Instead, because the service providers have a duty of precautionary storage of all telecommunications traffic data, and at the same time these data are released to be used by the police and the intelligence services as part of almost all their tasks, a data pool is created open to manifold and unlimited uses to which – restricted only by broad objectives – recourse may be had, in each case on the basis of decisions of the Federal and *Länder* legislatures. The supply of such a data pool with an open purpose removes the necessary connection between storage and purpose of storage and is incompatible with the constitution (see above C V 5 a). 285

In contrast, there is no objection to the fact that § 113b TKG contains no comprehensive provisions on duties of notification or on judicial review for the case where data stored under § 113a TKG are used to the purposes of warding off danger and of the carrying out of their duties by the intelligence services. 286

Admittedly, such provisions are constitutionally essential. However, the Federal legislature was entitled to leave these provisions connected with the retrieval of the data to be formulated in each case by the specialised legislation and thus, where appropriate, also by *Land* legislation.

c) Another aspect under which the formulation of the use of data stored under § 113a TKG is disproportionate is that there is no protection whatsoever of confidential relationships with regard to the transmission. At least for a narrowly defined group of telecommunications connections which rely on particular confidentiality, such a protection is fundamentally required (see above C V 2 e, at the end). 287

4. Finally, § 113b sentence 1 half-sentence 2 TKG, which provides for an indirect use of the data stored under § 113a TKG for information of the service providers under § 113.1 TKG, also does not satisfy the requirements of proportionality in every respect. 288

By the standards developed above, however, there are no constitutional objections to the fact that in § 113b sentence 1 half-sentence 2 TKG the legislature does not subject information on the owners of particular IP addresses already known to the authorities to the particularly stringent requirements which have to be satisfied for a direct retrieval of the data stored under § 113a TKG. It is therefore unobjectionable that under § 113b sentence 1 half-sentence 2 TKG in conjunction with § 113.1 TKG such information is permissible, without a prior judicial order, for the prosecution of criminal offences of every kind and in general for the tasks of warding off danger and of the intelligence services. However, the provision is not quite unambiguous with regard to the necessary encroachment thresholds. But when it is interpreted in conformity with the Basic Law, it can be understood to the effect that § 113.1 TKG refers to the relevant bases for encroachment in the specialised legislation, and that for access to the data it requires at least sufficient probable cause under §§ 161, 163 StPO or a concrete danger within the meaning of the blanket clauses in *Länder* police law (see Bock, in: Geppert/Piepenbrock/Schütz/Schuster, *Beck'scher Kommentar zum TKG* , 3rd ed. 2006, *§ 113* , marginal no. 7; Graulich, in: Arndt/Fetzer/Scherer, *TKG* , 2008, *§ 113* , marginal no. 8). For information requests by the intelligence services too, the encroachment threshold of the concrete danger must be derived from the provision, interpreted in conformity with the Basic Law. 289

Any abuse of the provision to circumvent § 100g StPO may also be countered by the way of interpretation in conformity with the Basic Law. Understood in the sense of the Basic Law, § 113b sentence 1 half-sentence 2 in conjunction with § 113.1 TKG does not authorise open retrieval by the authorities of the names of owners whose telecommunications connections are not known to them. Instead, corresponding to its objective as expressed in the legislature's statement of intention, it permits only information on individual IP addresses already known to the authorities (see Bundestag printed matter 16/6979, p. 46). In the necessary reform of the law, the legislature may review whether it finds occasion to clarify this by statute. In this connection, however, § 113b sentence 1 half-sentence 2 in conjunction with § 113.1 TKG is not found to be unconstitutional. 290

Nevertheless, § 113b sentence 1 half-sentence 2 in conjunction with § 113.1 TKG is too broad from the aspect of proportionality in that in general it regards the punishment of regulatory offences too as sufficient to justify such retrieval. Admittedly, under the standards developed above, the legislature is not as a matter of principle prevented from employing such information even in the field of regulatory offences in particularly important cases (see above C V 4 c). However, this requires special well-defined provisions, which are lacking in the present statute. In addition, § 113b sentence 1 half-sentence 2 in conjunction with § 113.1 TKG is also unconstitutional in that there are no provisions for notification of the persons affected. Under § 113.1 sentence 4 TKG, the persons with a duty to give information must observe secrecy towards the persons affected, and there is also no guarantee that the authorities seeking information will be notified. This does not satisfy the constitutional requirements of transparent use of the data stored under § 113a TKG (see above C V 3 a). 291

5. In summary, neither the framework established by law for data security nor the provisions on the use of data under § 113b sentence 1 no. 1 TKG in conjunction with § 100g StPO, § 113b sentences 1 nos. 2 and 3 TKG and § 113b sentence 1 half-sentence 2 TKG satisfy the constitutional requirements. Consequently, the duty of storage under § 113a TKG itself also lacks a constitutionally workable justification. The challenged provisions are therefore in their totality incompatible with Article 10.1 GG. 292

VII.

In contrast, the challenged provisions do not give rise to any constitutional objections with regard to Article 12.1 GG, to the extent that a decision has to be made in these proceedings in this respect. The occupational freedom of the fourth complainant in the proceedings 1 BvR 256/08 is not violated by the challenged provisions and the associated financial burden. 293

1. However, the imposition of duties of storage which affect the complainant at least insofar as it itself operates a publicly accessible anonymisation service, is an encroachment upon its occupational freedom. As the commercial supplier of an anonymisation service, it may invoke occupational freedom under Article 12.1 GG. In addition, the provision has an objective tendency to regulate an occupation or profession. The duties of storage are addressed to such service providers as generally offer publicly accessible telecommunications services for end users in return for payment (see § 113a.1, § 3 no. 24 TKG) and therefore to service providers which at all events typically offer the services for commercial purposes. 294

The encroachment is the regulation of the practice of an occupation or a profession. § 113a TKG provides for a duty of storage, and in § 113b sentence 1 half-sentence 1 TKG for a duty of transmission; these duties are presented as technical requirements for the provision of telecommunications services. In contrast, when it is submitted that the duty of storage has the effect of the regulation of a choice of occupation on anonymisation services because it is no longer possible to offer absolute anonymisation, this is mistaken. It is true that the regulation of a choice of occupation comes into consideration not only when access to an occupation or profession is legally restricted, but also when the meaningful exercise of an occupation or profession is effectively made impossible (see BVerfGE 30, 292 (313)). However, the duty of storage under § 113a.6 TKG does not result in it being fundamentally no longer possible to operate anonymisation services. The anonymisation services may continue to offer their users the possibility of surfing the Internet without the possibility of their IP addresses becoming known to private persons. In this way they make it possible for users who have a static (and therefore open) IP address to conceal their identity, and they protect other users against hackers or other illegal access. The anonymity is only lifted vis-à-vis the state authorities, and here only if a retrieval of data is exceptionally permitted under the narrow requirements for the direct use of the traffic data stored under § 113a. This therefore only deters customers whose interest in anonymisation is directed towards the authorities which conduct investigations in particularly serious cases. This does not vitiate the offer of an anonymisation service in its entirety. 295

2. The encroachment created by the imposition of the duties of storage is constitutionally justified. It is not disproportionate, either with regard to the technical effort or with regard to the associated financial burdens. 296

Encroachments upon the freedom to practise an occupation or a profession must be justified by sufficient reasons of the public interest (see BVerfGE 94, 372 (390); 101, 331 (347); 121, 317 (346)). Here, in principle, rational reasons of general welfare are sufficient (see BVerfGE 7, 377 (405-406); 16, 286 (297); 81, 156 (189); established case-law). Here too the requirements of the principle of proportionality apply, that is, the encroachment must be suitable to achieve the objective of the encroachment, necessary and proportionate in the narrow sense. These requirements are satisfied in the present case. 297

a) The duties of storage and transmission are also justified with regard to the encroachment upon occupational freedom by the objective of increasing the effectiveness of criminal prosecution, of warding off danger and of the duties of the secret services. They are thus based on rational reasons of general 298

welfare, which they are suitable to promote. A less encroaching provision that is as effective and is cost-effective for the state is not apparent. Since the privatisation of the telecommunications sector, telecommunications traffic data are no longer collected by the state, and therefore the state itself is not in the position to store data directly. A transmission of all connection data to the state in order that the state itself stores them is out of the question, in the first instance because of the risks entailed both for the protection of telecommunications secrecy and for the security and completeness of the data. In addition, when there are adverse effects on an occupation as the result of the imposition of cost burdens or costly obligations, the necessity does not cease to apply simply because financing the relevant task from public funds would be a more lenient means for those affected (see BVerfGE 81, 156 (193-194); 109, 64 (86)). More lenient means are not those which merely shift a cost burden (see BVerfGE 103, 172 (183-184); 109, 64 (86)).

b) The imposition of a duty of storage is not typically excessively burdensome for the service providers affected. 299

aa) The duty of storage does not cross the boundary of permissibility by reason of the technical effort it requires from the service providers. Since the service providers in question are actors on the telecommunications market, they must in any case display a high degree of mastery of technology in the area of the collection, storage and processing of telecommunications data. Even small enterprises in this sector must have these abilities. In addition, at all events a large part of the data to be stored under § 113a TKG are in any case temporarily stored by the relevant telecommunications enterprises for their own purposes. Exacting organisational requirements for the guarantee of data security do not arise merely from the duty of storage of § 113a TKG, but independently of this from the subject matter of the services offered by the relevant enterprises. In this respect, the imposition of the specific duties under § 113a TKG is not disproportionate from a technical and organisational point of view. 300

bb) Nor is the duty of storage disproportionate with regard to the financial burdens incurred by the enterprises as a result of the duty of storage under § 113a TKG and the duties consequential on this, such as the guarantee of data security. In particular, this is not unreasonable because as a result private enterprises would impermissibly be entrusted with state functions. A categorical separation of “state functions” and “private functions”, with the result that it would be impermissible to commission private persons for the purposes of public interest at their own cost, cannot be derived from the Basic Law. On the contrary, the legislature has a broad discretion as to what duties to ensure public interests it will impose on private persons in their work (see BVerfGE 109, 64 (85)). In principle, it may impose burdens and measures to safeguard public interests for which legislation is necessary as a result of commercial activities on the relevant actors in the market, in order in this way to integrate the associated costs in the market and the market price. Here, the legislature is not restricted to engaging private persons only if their occupation may directly cause dangers or if they are directly liable for these dangers. Instead, it is sufficient in this connection if there is a close relationship in subject-matter and in terms of responsibility between the person’s occupation and the duty imposed (see BVerfGE 95, 173 (187)). 301

There are therefore no fundamental objections to the cost burdens incurred by the persons with a duty of storage. In this way, the legislature shifts the costs associated with the storage as a whole onto the market, corresponding to the privatisation of the telecommunications sector. Just as the telecommunications enterprises can use the new opportunities of telecommunications technology to make profits, they must also assume the costs of containing the new security risks that are associated with telecommunications and must include them in their prices. The duties imposed on the enterprises are closely connected to the services rendered by them and can as such only be performed by themselves. In addition, it is not the case here that special sacrifices are imposed on individual service providers, but instead the basic conditions of the provision of telecommunications services are structured in a general way. It is thus constitutionally unobjectionable if the enterprises then also in principle bear the costs incurred by this. Reimbursement is not required to be provided merely because the objective relates to the public interest (see BVerfGE 30, 292 (311)). A statute which governs the practice of an occupation in such 302

a way that it imposes duties on private persons in the exercise of their occupation and in doing so normally affects a large number of persons is not disproportionate simply because it unreasonably burdens individual persons affected, but only if it violates the prohibition of disproportionate measures for a large group of persons affected (see BVerfGE 30, 292 (316)). As to the suggestion that the cost burdens arising in this manner have suffocating effects, this has neither been submitted with substantiation nor is it apparent.

It is therefore not necessary to review further whether with regard to particular groups of cases (see BVerfGE 30, 292 (327)) or special situations hardship provisions are necessary from the point of view of proportionality. For at all events the submissions of the fourth complainant in the proceedings 1 BvR 256/08 do not support this in any way. In particular, with regard to anonymisation services, the fourth complainant did not provide evidence of a burden exceeding that of the other telecommunications enterprises either for itself or for other providers of such services in a sufficiently comprehensible manner supported by specific figures. But it is only if this were done that it could be established that the scope of legislative discretion was exceeded when the anonymisation services were engaged. As long as the legislature's assessment is called into question only by assumptions and allegations, the Federal Constitutional Court cannot pursue this question (see BVerfGE 114, 196 (248)). 303

Nor is the duty of transmission under § 113b sentence 1 no. 1 TKG in conjunction with § 100g StPO subject to any fundamental objections with regard to possible remaining cost burdens; the legislature has provided provisions on compensation in this connection (see § 23.1 Court Payment and Reimbursement Act (*Justizvergütungs- und -entschädigungsgesetz* – JVEG). the claims for reimbursement here provided are not the subject of the present proceedings. 304

VIII.

Apart from this there are also no more extensive requirements of the challenged provisions arising from the fundamental rights, insofar as the violation of those rights has been permissibly challenged. 305

IX.

The violation of the fundamental right to protection of the secrecy of telecommunications under Article 10.1 GG makes §§ 113a and 113b TKG void, as it does § 100g.1 sentence 1 StPO insofar as traffic data under § 113a TKG may be collected under this provision. The challenged norms are therefore to be declared void, their violation of fundamental rights having been established (see § 95.1 sentence 1 and § 95.3 sentence 1 of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz* – BVerfGG). Accordingly, the telecommunications traffic data collected by the service providers under requests for information on the basis of the temporary injunction of 11 March 2008 and 28 October 2008 but provisionally not transmitted to the requesting authorities, which are stored, must be deleted without delay. They may not now be transmitted to the requesting agencies. 306

The decision on the reimbursement of expenses is based on § 34a.2 of the Federal Constitutional Court Act. 307

With regard to the questions of European law, the formal constitutionality and the fundamental compatibility with the Basic Law of the precautionary storage of telecommunications traffic data, the decision is unanimous. With regard to the assessment of §§ 113a and 113b TKG as unconstitutional, it was passed by seven votes to one as regards its result, and with regard to further questions of substantive law it was passed by six votes to two, to the extent shown in the dissenting opinions. 308

The Senate decided by four votes to four that the provisions are to be declared void under § 95.3 sentence 1 of the Federal Constitutional Court Act, and not merely incompatible with the Basic Law. Accordingly, it is not possible for the provisions to continue in effect in a restricted scope; instead, the statutory consequence is an annulment. 309

Papier Hohmann-Dennhardt Bryde
Gaier Eichberger Schluckebier
Kirchhof Masing

Dissenting opinion of Justice Schluckebier

to the judgment of the First Senate of 2 March 2010

– 1 BvR 256/08 –

– 1 BvR 263/08 –

– 1 BvR 586/08 –

Due to the considerations outlined below, I cannot agree with the decision as regards its result and large parts of its reasoning. 310

The Senate holds that the storage of the traffic data has the effect of a particularly serious encroachment upon the fundamental right under Article 10 GG. In my view, particular weight must indeed be attributed to such an encroachment; as compared to content-related surveillance measures, however, it proves to be considerably less serious (on this, see I.). In view of the objectives pursued by the legislature, in particular the investigation of criminal offences that even in an individual case are of substantial importance or have been committed by means of telecommunications but are difficult to investigate, I furthermore regard the encroachment caused by the storage of the traffic data and by the provisions on access under the law of criminal procedure as fundamentally justified under constitutional law. In my view, the provisions on which the encroachment is based essentially stand up to a review of proportionality in the narrow sense, and especially to a review of appropriateness and reasonableness (on this, see II.). Merely the requirements in terms of content placed on the guarantee of the data security of the telecommunications traffic data to be stored and transmitted are excluded from this; in this respect, I concur with the majority of the Senate, without taking up this aspect again in the following. As regards the pronouncement of the legal consequences, the challenged provisions should, on the basis of the Senate majority's evaluation, not have been declared void in my view; in accordance with the temporary injunctions issued by the Senate, they should have been regarded as applicable until the adoption of new provisions (on this, see III.). 311

I.

The majority of the Senate considers the storage of the traffic data by the service providers for a period of six months as a particularly serious encroachment upon the fundamental right of Article 10.1 GG. I do not agree with this weighting. 312

The secrecy of telecommunications protects the contents and the circumstances of the act of communication against *state authority gaining knowledge of them* (see BVerfGE 100, 313 (358); 106, 28 (37); 107, 299 (312-313)). If the private service providers' obligation to store data (§ 113a TKG) is ascribed the nature of an encroachment because the service providers are "helpers of the state" and the storage must therefore be attributed to the state, the circumstance that before a possible access by state agencies, the data exclusively remain in the sphere of the private service providers attains special importance for the assessment of the intensity of the encroachment. The data are in the hands of the party to the contract on which those who make use of the services place the fundamental confidence, which must be assumed where contracts of this kind are concluded, that this party will treat the data that arise for operational reasons and for billing with strict confidence and guarantee their protection. If, furthermore, an appropriate, state-of-the-art level of data security is guaranteed, there is thus also no objectifiable basis for the assumption that the citizen could feel intimidated as a result of the storage, which would increase the intensity of the encroachment, or, in the words of the judgment, of a "sense of being permanently 313

monitored" and of a "diffuse sense of threat". Moreover, storage does not take place secretly but on the basis of a law that has been made public. The object of the storage is not the *contents* of acts of telecommunication. Insofar as the traffic data, to a limited extent, also permit conclusions regarding such contents or even make it possible to track people's movements or to create social profiles, this concerns the issue of the proportionality of the corresponding provisions on access and of the compliance with the requirements of proportionality on the level of the application of the law. The fact that such uses, which can constitute an intensive encroachment in individual cases, are possible if sufficiently weighty reasons exist does not justify attaching to such uses, which in an overall assessment prove to be exceptional cases, decisive importance in the weighting of the storage and to unrestrictedly base the weighting on them.

314 In its judgment of 12 March 2003 (BVerfGE 107, 299 (322)) on the *delivery* of telecommunications connection data which referred to telephone calls, the Senate already emphasised that the weight of the encroachment – in that case, of the encroachment caused by the data retrieval – was minor than that of telephone surveillance related to the contents of communication but that it was nevertheless high. It is true that the circumstances of the present case are special as regards the far-reaching effects and the precautionary character of the obligation to store data. However, when the encroachment is weighted, a perceptible distance must be observed to particularly serious encroachments such as those that occur in the acoustic surveillance of living quarters, in the online search of IT systems, but also in the monitoring of the contents of telecommunications and their evaluation *by the direct access of state bodies* ; in the case of these encroachments, there is a particular risk that the core area of private life, which enjoys absolute protection, is affected, something which is not the case with the encroachments dealt with here. However, from the perspective of the individual subject of fundamental rights who is affected, the collection of the traffic data of all telecommunications contacts by the private service providers without state authority gaining knowledge of them, and the possibility of their retrieval, which is provided separately under strict substantive preconditions, retrieval which, as a general rule, is revised, on the level of the application of the law, by the judge ordering the storage and is strictly limited, and takes place under procedural safeguards such as the ones provided for data collection pursuant to § 100g StPO, do not constitute an encroachment upon fundamental rights encroachment which is of such weight that it would be justified to classify it as "particularly serious" and thus as one of the greatest encroachments on the fundamental right which are imaginable. What remains, accordingly, is an encroachment due to the storage by the private service provider which can be characterised as particularly weighty. This differentiation attains its ulterior significance with regard to the review of the appropriateness of the challenged provisions.

II.

315 In derogation of the Senate majority's assessment, the challenged provisions on the duty to store traffic data and to collect them for purposes of the prosecution of criminal offences are not inappropriate, and they are reasonable for the persons affected and thus proportionate in the narrow sense.

316 1. The provisions take sufficient account of the precept of appropriateness and of reasonableness as a result of the principle of proportionality. On the basis of an overall weighing of the seriousness of the encroachment upon Article 10.1 GG and the weight of the reasons that justify it, it becomes apparent that the legislature has respected the limits resulting from this precept.

317 The precept of proportionality in the narrow sense requires that in an overall assessment, the seriousness of the encroachment may not be out of proportion to the weight of the reasons justifying it (see BVerfGE 90, 145 (173); 92, 277 (327); 109, 279 (349 et seq.); 115, 320 (345)). In the conflicting relationship between the state's duty to protect legal interests and the individuals' interest in the safeguarding of their rights guaranteed by the constitution, it is the initial task of the legislature to proceed in an abstract manner and achieve a balance between the conflicting interests (see BVerfGE 109, 279 (350); 115, 320 (346)). In doing this, it has latitude for assessment and drafting, something the majority of the Senate also essentially assumes according to its choice of terminology.

When assessing the appropriateness of the provision under constitutional law, one has to consider, as a starting point, that the fundamental rights are not confined to warding off state encroachment. Due to their objective-law dimension, the duty of the state to protect the citizens from their rights being infringed results from them. This duty to protect includes the duty to take suitable measures in order to prevent injury to legal interests or to investigate such injury if necessary, to attribute responsibility for injuries to legal interests and to restore legal peace (see Jutta Limbach, *Anwaltsblatt* – AnwBl 2002, p. 454). In this sense, guaranteeing the protection of citizens and of their fundamental rights and the foundations of the community, and the prevention and investigation of serious criminal offences, are all among the requirements for peaceful coexistence and the citizens' untroubled enjoyment of their fundamental rights. The effective investigation of crimes and effective warding off of danger are therefore not in themselves a threat to the freedom of citizens; they are however, impermissible without any restraints and limits. They are indicated within the bounds of what is appropriate and reasonable in order to secure that *inter alia* the fundamental rights are made use of and in order to protect the individual's legal interests. In the state under the rule of law, the citizen must be able to rely on effective protection by the state just as much as on protection against the state (see Di Fabio, *Neue Juristische Wochenschrift* 2008, p. 421 (422)). Accordingly, the Federal Constitutional Court has described that state as power guaranteeing peace and stability under the constitution (*verfasste Friedens- und Ordnungsmacht*) and has recognised the security of its citizens, which it must guarantee, as a constitutional value that is of equal rank with other such values and is indispensable because the state as an institution derives its justification *inter alia* from it (see BVerfGE 49, 24 (56-57); 115, 320 (346)). 318

As regards the balancing of the conflicting interests by the legislature, which must create the legal foundations for the investigation of criminal offences and for warding off danger, it must furthermore be taken into account that it is reasonable to expect the individuals, as regards their relation and their commitment to the community, to tolerate certain impairments which serve the protection of other citizens' legal interests and fundamental rights, but also the individuals' own protection (see BVerfGE 4, 7 (15); 33, 303 (334); 50, 166 (175)). Also with a view to this, the legislature must be granted discretion for the balancing which is its duty, so that it can protect, on the one hand, the liberty rights of the subjects of fundamental rights, while creating, on the other hand, the legal framework conditions which make it possible to ensure an effective legal protection of the citizen's legal interests and fundamental rights against injury, and to investigate criminal offences, with appropriate and reasonable means. 319

2. In establishing the duty to store telecommunications traffic data for a period of six months, a provision as to the purpose of use and a criminal-procedure provision for collection of data, the legislature has remained within the legislative limits accorded to it under the constitution. With a view to the fundamental rights and legal interests to be protected, the impairment of the telecommunication participants affected by the storage of traffic data is not inappropriate and unreasonable; on the other side of the balance which must be found are the legislative weighting of the protection of the legal interests of individuals and of the general public which are injured by criminal offences and the warding off of dangers in this respect in an age of a very far-reaching expansion of the possibilities of electronic communication, which often leaves little or no trace. This view is basically held by the majority of the Senate as well; however, it only takes this aspect into account when evaluating the question of the suitability and necessity of the provisions without explicitly integrating it into a review of appropriateness which really sees the interests affected "in relation to each other". 320

a) The latitude for drafting which the legislature primarily has when establishing a balance, in an abstract manner, between the legal and other interests in the conflicting relationship of "freedom and security" (see BVerfGE 109, 279 (350); 115, 320 (346)) is also influenced by the special character of the subject-matters which are to be regulated, and by the reality to which the provision must do justice. Therefore, the purpose and the effectiveness of the provisions must also be taken into account when assessing appropriateness and reasonableness. 321

322 Through the Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation and for the Implementation of Directive 2006/24/EC, the legislature fundamentally changed the system of the methods of undercover investigation under the law of criminal procedure. In doing so, it proceeded with great care, relying on expert opinions requested by it, on an extensive discussion among legal scholars, and also on empirical reports from the public prosecution authorities and police authorities (see Bill, Bundestag printed paper 16/5846, p. 1). Detailed hearings of experts took place in the parliamentary procedure (see the records of the 73rd and 74th meeting of the German Bundestag's Committee on Legal Affairs, 16th electoral term, on 19 and 21 September 2007). Moreover, it was intended to implement the Federal Constitutional Court's case-law existing to date. Finally, the Act was approved by a very broad majority (see Minutes of plenary proceedings of the German Bundestag, 16th electoral term, 124th session on 9 November 2007, p. 13009 (D); see also the speech by Federal Minister of Justice Brigitte Zypries introducing the bill, *loc. cit.* , Minutes of plenary proceedings pp. 12994-12995). The legislature intended to take new technical developments into consideration because it considered precisely the measures at issue here particularly effective in the investigation especially of crime that is difficult to investigate, of transaction crime, white-collar crime and criminal offences committed using modern communication technologies (see Bill, Bundestag printed paper 16/5846, p. 2). Furthermore, it was [the legislature's] declared goal to take account of the irrefutable needs of an effective, constitutional administration of criminal justice, whose task it is to achieve justice and legal peace within the limits that are set to it. This goal cannot be achieved unless the facts necessary for the investigation can be ascertained (*loc. cit.* , p. 22). In this connection, the legislature assumed that telecommunications traffic data above all, because of the technical development towards more flat-rate connections – and unlike in the past, when especially call data regarding telephony were available for many months –are either not stored at all or are deleted before a judge's order for the issuing of information can be obtained, or even before the information necessary for an application for such an order has been ascertained (*loc. cit.* , p. 27). Apart from this, it is generally known that criminal offences are committed on and through the Internet itself. Reality in society, which includes the existence of crime, is reflected also in this context in the different branches of telecommunication. If the legislature reacts on this, but if what is necessary according to its assessment is only possible in an efficient manner if the corresponding traffic data are subject to an obligation of storage for a certain period of time which the legislature imposes on the service providers, this is essentially not inappropriate, and it is reasonable for the subjects of fundamental rights whose data are concerned. Such provision exists in other areas of the legal system as well, for example, without this being directly comparable, in the field of the obligations of residents to register or as regards the retention of what is known as master account data by the banks (on this see § 24c of the Banking Act (*Kreditwesengesetz* – KWG); BVerfGE 118, 168).

323 The activity report 2008/2009 of the Federal Network Agency, which shows the development of the number of different types of access to voice and other data communication in recent years, confirms in a certain way that the approach chosen by the legislature is not unbalanced. The report impressively proves the enormous rates of increase of lines but above all of the volumes of speech and data exchanged in the network. It proves that a fundamental change of the communicative behaviour of people has taken place in recent years (see *loc. cit.,* for example p. 38 on digital subscriber lines, p. 50 on the subscriber development in mobile telephone networks, p. 53 on the speech volume in mobile telephone communication and the rates of increase in flat rate billing, p. 59 on the volume of traffic via broadband lines).

324 Under these circumstances, the legislature, in order to protect the legal interests of the victims of criminal offences, essentially cannot be denied taking the effectiveness of the means provided by it into consideration and to adapt to the changed situation also by obliging the service providers to store and retain traffic data in their sphere for a certain period of time. In this context, the state bodies' keeping pace with technical progress cannot merely be seen as something which rounds off the arsenal of methods of criminal investigation in a sensible manner, and which complements conventional investigation methods that remain effective; instead, it must be seen against the backdrop of the shift of conventional forms of

communication towards electronic information traffic including its subsequent digital processing and storage. For the effective prosecution of criminal offences and warding off of danger not only in the area of serious crime but also for the investigation of criminal offences that even in an individual case are of substantial importance or have been committed by means of telecommunications but are difficult to investigate without access to traffic data, the availability of the traffic data for a period of six months is, according to the legislature's unobjectionable assessment, of great importance (see BVerfGE 115, 166 (192 et seq.); see also BVerfG, First Chamber of the Second Senate, order of 22 August 2006 – 2 BvR 1345/03 –, *Neue Juristische Wochenschrift* 2007, p. 351 (355)).

Accordingly, also the majority of the Senate acknowledges that the increased use of electronic or digital means of communication and their invading virtually all areas of life makes the prosecution of criminal offences and also the warding off of danger more difficult and that modern communications technologies are increasingly used in connection with a wide variety of crimes and that they contribute to also making criminal acts more effective. In the review of proportionality in the narrow sense it does not attach this development the weight that is necessary in my view. 325

b) What is more, as regards the practical result, the majority of the Senate virtually completely restricts the legislature's latitude for assessment and drafting, which would permit it to pass appropriate and reasonable provisions in the field of the investigation of crimes and the warding off of danger for the protection of the population. In this way it also fails to take sufficient account of the requirement of judicial self-restraint with regard to conceptual decisions of the democratically legitimated legislature. It prescribes the legislature the details of a statutory regulation in the manner of an instruction to act which leaves virtually no room for a solution that, according to the legislature's assessment, takes account of the existing circumstances in the area of telecommunications and the change that they have undergone. 326

The judgment finds that a storage duration of six months – that is, the minimum period called for by the EC Directive – is at the upper limit and at best capable of being constitutionally justified; it dictates to the legislature the technical rule that the provision on the purpose of use must at the same time contain the requirements for access, restricts the legislature to providing for lists of offences in criminal law, excludes the possibility of using the traffic data even to solve criminal offences that are difficult to investigate and were committed by use of the means of telecommunications, and extends the duties of notification in a specific manner. Following this, the legislature no longer has an appreciable discretion to legislate on its own political responsibility. It is essentially restricted to slightly adapting and modifying peripheral sectors of the list of criminal offences which justify data retrieval under the law of criminal procedure. It must implement the judgment unless it intends to refrain from passing a new provision, which would be contrary to Community law. Thus the judgment, as regards its practical result, *substitutes* legislation in that it even prescribes the details of a provision which the Senate regards as the only one that is constitutionally permissible. 327

3. The majority of the Senate demands that the legislature, when determining the purpose of use of the data, has to achieve clarity about the requirements for access and about procedural safeguard requirements. By doing so, it deprives the legislature of the possibility of operating, as regards the technical rules, with a system of complementary legal foundations, something which has not been objected to as yet in other areas. In what is known as its master account data decision, for example, the Senate has not found it constitutionally objectionable that the retrieval must be necessary to perform statutory duties which are provided elsewhere, that the cause of and the requirements for retrieval are, however, determined in a different Act (see BVerfGE 118, 168 (191)). However, in its decision on what is known as automatic number plate recognition, the Senate regarded the indications concerning the purpose of use as insufficient; the challenged Act did not make a statement on the purpose of use, thus including all conceivable purposes of use (see BVerfGE 120, 378 (409)). This, however, is different here (§ 113b TKG). It therefore benefits precisely the clarity of statutory provisions if the legal preconditions and provisos which result in the considerable intensification of the encroachment by the retrieval of the data are provided for in an area-specific manner in independent systems of provisions that relate to the 328

respective legal area. As a matter of course, both provisions are subject to the constitutional requirements and constitutional review, if necessary, even as regards their interaction. Even if in relation to a *Land* legislature, the Federal legislature bears the responsibility of the storage of the traffic data, a possible provision under *Land* law which complements it must also comply with the constitution. Thus, no deficiency can occur as results legal protection.

Accordingly, there was no reason here to also deal, apart from the criminal-law provision on access 329
under § 100g StPO, which was challenged in part by the constitutional complaints, with the details of the requirements of the use of the traffic data for warding off danger and for intelligence-service purposes.

4. Finally, the Senate refuses the legislature the right to retrieve the traffic data to investigate criminal 330
offences that are not contained in the present list under § 100a.2 StPO but that are nevertheless of substantial importance in the individual case, and offences that are committed by means of telecommunications (§ 100g.1 sentence 1 nos. 1 and 2 StPO). In doing so, it also does not give due account to the weight of the possible offences and – to the extent that the legislature has considered them difficult to investigate – to the importance of the data for an effective investigation of criminal offences. With regard to no. 1 of § 100g.1 sentence 1 StPO, the legislature was guided by criteria which the Senate approved in its judgment of 12 March 2003 (BVerfGE 107, 299 (322)) on the release of telecommunications connection data. The Senate emphasised there that such encroachment is only justified with criminal offences to which the legislature generally attaches special weight and which are of substantial importance in the specific case, for example due to the damage caused and the degree of threat to the general public. I do not see that the threshold of encroachment which the Senate did not object to there would have to be weighted in a fundamentally different manner with regard to access to what is known as retained traffic data. In the combination of circumstances at issue there, the review of constitutionality in the individual case is incumbent on the judge ordering access; the judge has to include the weight of the access on the traffic data in the respective case in the weighing and has to limit it by the drafting of the order.

With regard to offences committed by means of telecommunications, for which the Senate would like to 331
have ensured that access to the traffic data which are stored according to § 113a TKG is excluded as well, insufficient weight is attached to the fact that the legislature assumes substantial difficulties in investigation here. Apart from the particular weight of the offence to be investigated, also those difficulties may make the retrieval of retained traffic data seem appropriate, especially if, as is the case here, the legislature has provided the conditions for retrieval with a strict subsidiarity clause according to which the measure is permissible only if the investigation of the facts or the establishment of the whereabouts of the suspect in another way would be impossible or considerably more difficult and if the collection of the data is in a reasonable proportion to the importance of the matter even in the individual case (§ 100g.1 sentence 2 StPO).

Since it is the duty of the legislature to guarantee effective criminal prosecution and not to permit any 332
substantial gaps in protection, the legislature may not be denied also giving access to the traffic data in the case of offences that may not be particularly serious if the legal interest injured is nevertheless of particular importance, because in its estimation this is the only way to prevent de facto legal vacuums and a situation where investigation is largely ineffective. Here, the legal offence of stalking, for example, may be cited as an example (§ 238.1 no. 2 StGB, “cyberstalking“); in this context, the traffic data are often the only investigative lead to verify statements in a situation in which it is one person’s word against another’s, but also to identify a perpetrator who is unknown at first. Here the possibility of using a telephone trap is helpful only to a limited extent because it does not cover the email traffic and ultimately depends on the service providers’ goodwill. Something similar applies to the offence of threatening the commission of a felony, above all, however, to the area of internet fraud, which, according to the crime statistics compiled by the police, involves a considerable number of cases. Finally, access to traffic data may be a consideration also with regard to other offences (§ 202a to 202c StGB, data espionage and phishing; see also §§ 269, 303a, 303b StGB, forgery of data intended to provide proof, data tampering, computer

sabotage; § 38.1 of the Securities Trading Act (*Wertpapierhandelsgesetz* – WpHG) in conjunction with § 14.1 no. 1 WpHG, so-called insider trading, § 38.2 in conjunction with § 39.1 no. 1, § 20a.1 sentence 1 nos. 1 to 3 WpHG, illegal manipulations of the market; § 86 StGB, dissemination of propaganda material of unconstitutional organisations).

Admittedly, it seems conceivable that the legislature will incorporate some of these offences into the list of serious criminal offences demanded by the Senate. In doing so, however, it will come up against the limits of an appropriate threat of punishment committed to the principle of guilt which can justify this measure. It will thus hardly be permitted to incorporate, for example, offences which are not committed for commercial purposes or do not cause major damage in an individual case into a list such as the one which the Senate is contemplating. It will hardly be possible to mitigate the deficiencies in investigation by making use of non-retained data which only exist for technical reasons. Experience has shown that great differences exist between the service providers in this respect. In some cases, data are not retained at all, in other cases they are already deleted after a few hours or days. Even the investigation measures which will lead to the application for the issuing of a judicial order, the preparation of such an application and the decision on it will often take more time than the service provider keeps the data available for technical reasons. 333

5. Something similar applies with regard to the threshold of interference which the Senate establishes for purposes of warding off danger. The legal interests which the Senate considers sufficiently weighty for the traffic data to be regarded as retrievable and usable would have had to include the warding off of a danger, which is not at the same time a danger to public safety, to property of significant value, maintenance of which is demanded by the public interest. It does not seem plausible to me to exclude important material assets covered by this definition because they are also protected by fundamental rights (see Article 14.1 GG). To include this legal interest into protection as well is not inappropriate at least if the collection of traffic data furthermore contains a subsidiarity clause, as is the case for example in § 20m BKAG ("… would be impossible or considerably more difficult.") 334

6. To the extent that the majority of the Senate postulates an extension of the duties of notification for the case of access to traffic data and demands in principle, with regard to the law of criminal procedure, not only what is known as *open* access but notification "*before* the retrieval or transmission" if this does not run counter to the protection of the purpose of the investigation, this requirement also goes beyond the legislative concept, thereby interfering with the legislature's discretion. The concept of the legislature was to pass provisions on all "measures of *undercover* investigation", among which it expressly included the collection of traffic data (Bill, Bundestag printed paper BTDrucks 16/5846, p. 2). Also § 100g StPO provides that traffic data may (at first) be collected "without the knowledge of the person concerned". And this is with good reason. For as a general rule, investigations are characterised by a considerable dynamics and have to be conducted rapidly. Effort which purposes of procedural safeguarding and of the protection of the law do not absolutely demand to be made *within a narrow time frame* should *at first* be limited. Accordingly, the legislature has passed a differentiated provision on notification also for the collection of traffic data (see § 101.1, 101.4 sentence 1 no. 5, 104.5 StPO), which does not prescribe prior notification. In addition, the legislature, by permitting to collect traffic data at first without the knowledge of the person concerned, discernably introduced a categorisation which is due to the fact that in most cases, the purpose of the investigation, the unknown whereabouts of the person affected or the need to rapidly investigate the facts are contrary to prior notification. This is evidently not inappropriate, reasonable with regard to the person affected, and the legislature is therefore not constitutionally banned from proceeding in this manner. 335

III.

It is true that the declaration of nullity of the challenged provisions which was pronounced by the Senate is the legal consequence of the declaration of incompatibility which has been carried by the majority. However, on the basis of the constitutional assessment of the majority of the Senate, having recourse to 336

established case-law of the Federal Constitutional Court, consideration might well have been given to fixing a time limit for the legislature to pass new legislation and to holding that the existing provisions could provisionally continue in effect in conformity with the stipulations of the temporary injunctions granted by the Senate. For the Senate grants the legislature the possibility of providing for an obligation to store traffic data for six months and also of passing provisions on access, under the preconditions specified in the judgment, which essentially comply with the requirements made in the temporary injunctions. The stipulations of the judgment mainly differ from those of the temporary injunctions merely by establishing higher requirements with regard to data security and by demanding further-reaching obligations of notification. With a view to the weighing, the Federal Constitutional Court's frequent practice suggests to refrain at first from pronouncing a declaration of nullity and not to regard it as imperative to only permit, for the time being, the access to data of the service providers which still exist for technical or billing reasons. Thus considerable shortcomings in warding off danger and in the investigation even of serious criminal offences will have to be feared, and are tolerated, until the enactment of a new provision. Reference is made to the grounds of the temporary injunctions issued by the Senate and to the weighing made therein. In addition, the service providers must stay their measures implementing the challenged regulation and restore the previous situation, once the new, amended law will have been enacted, something which is required already under Community law, they will have to make considerable effort to create the requirements once again.

Schluckebier

Dissenting opinion of Justice Eichberger

to the judgment of the First Senate of 2 March 2010

– 1 BvR 256/08 –

– 1 BvR 263/08 –

– 1 BvR 586/08 –

I do not agree with the decision of the Senate majority with regard to part of the result of the judgment and with regard to essential elements of the reasoning. Basically, I agree with Justice Schluckebier's critcism of them, and I agree with most of his opinion concerning the conclusion and the reasoning. In the following, I can therefore restrict myself to giving a brief account of the considerations that are essential for my point of view: 337

1. Also in my view, the statutory order to store the telecommunications traffic data is a weighty encroachment upon Article 10.1 GG in view of its broad and comprehensive character in terms of the staff and resources involved, in view of the fact that it takes place without a cause and in view of the considerable length of time of the prescribed data retention. As, however, the obligation to store data is restricted to the traffic data and does not cover the contents of the acts of telecommunication, and as it takes place in a decentralised manner by the service providers, the encroachment that goes along with the storage does not have the overriding importance that is generally attributed to it by the majority of the Senate. In view of the legislative concept of the data storage, which rules out a free access by state authorities on the traffic data stored in a decentralised manner by the private service providers, and which provides for strict barriers in terms of content and with regard to the law of procedure – in particular a substantial requirement of judicial authority – to data retrieval or, in my view, has to be amended by such statutory requirements, I regard the fear expressed by the majority of the Senate of an intimidating effect on the communication behaviour of the population as unfounded, at any rate as not empirically proven. 338

Therefore, in my opinion, the essential burdening effect on the interest protected by Article 10.1 GG for the citizens that results from the ordering of the data storage is first and foremost due to the potential danger, emanating from this large collection of data, of abuse by the service providers themselves or by unauthorised third parties or of excessive use by prosecution or police authorities. Precautions must be taken against this. I therefore unreservedly agree with the view taken by the majority of the Senate concerning the standards for sophisticated data security to be prescribed to the service providers by the legislature. I also essentially agree with most of the other safeguards under procedural law for data storage, data retrieval and the further use of the data (obligations to delete data and obligations of recording, requirements concerning transparency and legal protection) which the majority of the Senate considers necessary; according to my assessment, however, the requirements which the majority of the Senate places on the legislature in this context are too detailed in many respects and do not take sufficient account of the discretion which the constitution grants the legislature also in this context. 339

2. Unlike the majority of the Senate, and concurring with Justice Schluckebier, I am of the opinion that the legislative concept on which §§ 113a, 113b TKG are based, creating a sliding scale of legislative responsibility for the order of storage and the retrieval of data, is fundamentally in conformity with the constitution. In the context of this concept, § 113b TKG does not establish an independent encroachment upon Article 10.1 GG that goes beyond the order of data storage in § 113a TKG. Instead, the provision contains the constitutionally required determination of the purpose of the storage of the traffic data. Only the statutory authorisation granted elsewhere to retrieve data, which is provided in § 113b sentence 1 TKG, results in a new encroachment upon Article 10.1 GG that goes beyond the significance of the data storage performed until then. In this manner, the Federal legislature, with § 113b TKG, leaves the legislature of the Federation or of the *Länder* that is competent for the respective area the authorisation, which is due to it by virtue of its constitutional and democratic legitimisation, to decide whether and to what extent it will access telecommunications traffic data for purposes of the prosecution of criminal offences, to ward off danger or for the duties of the intelligence services. In doing so, the respective legislature, as a matter of course, must respect on its own responsibility the constitutional boundaries of a proportionate access to the traffic data. 340

This does not constitute an order of collecting data to keep them in reserve for undetermined purposes, which would be constitutionally impermissible. While obliging the service providers in § 113a TKG to store data, the Federal legislature specified in § 113b TKG the purposes for which the stored data may be used. The responsibility, which the Federal legislature assumed by ordering the data storage, for the potential danger thus created to the detriment of the citizens in my view requires however, and in this I agree with the starting point of the opinion of the Senate majority, not only a fundamental outline of the purpose of use but also the determination of at least a minimum threshold of interference; such a threshold has been provided with regard to the prosecution of criminal offences in § 113b sentence 1 no. 1 TKG in conjunction with § 100g.1 StPO, which has been adopted at the same time, and has been described using the term “substantial dangers” in § 113b sentence 1 no. 2 TKG with regard to the warding off of dangers but has not been provided in a similar manner with regard to the performance of the duties of the intelligence services. An amendment to this effect would be required here. However, I do not regard a detailed and final determination of the purposes of use which the majority of the Senate demands from the Federal legislature to be made at the same time as the order of the data storage as constitutionally required. 341

3. Finally, and above all, I cannot agree with the result of weighing reached by the majority of the Senate to the extent that it regards the use of the data stored under § 113a TKG, which is governed by § 100g StPO, for purposes of criminal prosecution as unconstitutional. The reason for this is, firstly, that the majority of the Senate, already in the starting point of its considerations, attaches, in my opinion, too much weight to the encroachment upon Article 10.1 GG caused by the ordering of the data storage and, in contrast, too little importance to the justified interest of the general public and of the individual citizens in an effective prosecution of criminal offences and in an effective warding off of dangers. Moreover, it places 342

too little value on the margin of discretion which is due to the legislature when evaluating the conflicting legal interests that merit protection and the drafting of the provision. On this point, I make reference to the statements made by Justice Schluckebier in his dissenting opinion, to which I agree.

Apart from this, the review of proportionality performed by the majority of the Senate suffers from its always assuming the greatest possible encroachment of a comprehensive form of data retrieval which ultimately aims to create a social profile of the citizen affected or to track his or her movements. This can indeed constitute an encroachment whose seriousness is similar to that of a weighty access to the contents of a citizen's acts of telecommunication. This perspective, however, leaves out of account that many instances of data retrieval may concern individual events, short periods of time and the telecommunications contacts of only one, or few, persons (for example the telecommunications connections of one person in one day or even in a specific hour). The weight of the encroachment that such data retrieval constitutes is minor; it is not comparable, at any rate, to access to contents of communication, regardless of the fact that the retrieval draws on the comprehensively compiled data collection. By regarding every data retrieval as a particularly serious encroachment upon Article 10.1 GG, irrespective of its concrete extent in the individual case, and thus generally considering the legislature constitutionally obliged to establish very high thresholds of encroachment, the majority of the Senate, in my view, also gets into a conflict of evaluation, even though it denies this, because it is possible for the authorities to retrieve similar data, without the Senate objecting, if they are not stored by the services provider according to § 113a TKG but for technical reasons. 343

On this basis, I can, in spite of the different weighting, still concur with the starting point of the conditions, for which the majority of the Senate has established standards, of a permissible use of the traffic data for warding off danger and for intelligence-service purposes (C V 2 b and c) but not with the requirements which the majority of the Senate places on the use of the data for the prosecution of criminal offences (C V 2 a and C VI 3 a aa). In this respect, I regard the differentiated concept for the collection and use of data for criminal prosecution created by the legislature in § 100g StPO as constitutional. It is the duty of the judge competent to decide on the permissibility of a retrieval of data in every individual case to take due account of the legal interests worthy of protection under Article 10.1 GG considering the weight of the respective encroachment, as is explicitly demanded from the legislature particularly as regards the criminal offences committed by means of telecommunications in § 100g.1 sentence 2 StPO. 344

4. In my opinion, even from the point of view of the majority of the Senate, merely the unconstitutionality of the challenged provisions would have had to be established and according to the temporary injunctions issued in this matter, at least the data collection and storage in the interim until the passing of a new, constitutional provision would have had to be ordered. By declaring the provisions void without transition and by establishing an obligation to delete the traffic data obtained on the basis of the temporary injunctions, the majority of the Senate tolerates disadvantages for the prosecution of criminal offences but above all the risk of dangers, which cannot be excluded, to important legal interests that must be protected even though it regards instances of data retrieval which meet the requirements formulated in the temporary injunctions as fundamentally constitutional and a corresponding legal regulation is to be expected. I cannot concur with such a solution. 345

Eichberger