

Headnotes  
to the Order of the First Senate  
of 24 January 2012  
– 1 BvR 1299/05 –

- 1. The attribution of telecommunications numbers to their subscribers is an encroachment upon the right to informational self-determination. In contrast, the attribution of dynamic IP address is an encroachment upon Article 10.1 of the Basic Law (Grundgesetz – GG).**
- 2. When creating an information procedure, the legislature must create a legal basis both for the transmission and for the retrieval of data.**
- 3. The automated information procedure under §§ 112, 111 of the Telecommunications Act (Telekommunikationsgesetz – TKG) is compatible with the constitution. In this connection, § 112 TKG requires independent enabling legislation for the retrieval.**
- 4. The manual information procedure of §§ 113.1 sentence 1, 111, 95.1 TKG is compatible with the Basic Law when interpreted in conformity with the constitution. Firstly, an appropriate legal basis is necessary for the retrieval of the data, and this legislation must itself have clear definitions creating a duty of information of the telecommunications enterprises. Secondly, the provision may not be used to attribute dynamic IP addresses.**
- 5. The security authorities may only require information on access codes (§ 113.1 sentence 2 TKG) if the statutory requirements for their use are satisfied.**



**IN THE NAME OF THE PEOPLE**

**In the proceedings  
on  
the constitutional complaint**

1. of Mr. B...,

2. of Mr. B...,

- authorised representative: Meinhard Starostik, attorney,  
Schillstraße 9, 10785 Berlin –

against 95.3 and 95.4, §§ 111, 112, 113 of the Telecommunications Act (Telekommunikationsgesetz – TKG) of 22 June 2004 (Federal Law Gazette (Bundesgesetzblatt – BGBl) I p. 1190)

the Federal Constitutional Court – First Senate – sitting with the justices

Vice-President Kirchhof,  
Gaier,  
Eichberger,  
Schluckebier,  
Masing,  
Paulus,  
Baer, and  
Britz

held as follows on 24 January 2012:

1. § 113.1 sentence 2 of the Telecommunications Act of 22 June 2004 (Federal Law Gazette I page 1190) is incompatible with Article 2.1 in conjunction with Article 1.1 of the Basic Law (Grundgesetz – GG).

For a transitional period, but at the latest until 30 June 2013, the provision shall continue in effect subject to the proviso that the data named in the provision may only be collected if the statutory requirements for their use are satisfied.

2. To the extent that the constitutional complaint challenges § 113.1 sentence 1 of the Telecommunications Act of 22 June 2004 (Federal Law Gazette I page 1190), it is rejected as unfounded, subject to the proviso that the provision is to be interpreted constitutionally in conformity with the grounds of this decision (C. IV. 1.-3.) and thus only in conjunction with an appropriate legal basis for the data retrieval and may not be used for the attribution of dynamic IP addresses.

For a transitional period, but until 30 June 2013 at the latest, the provision may also be applied independently of these conditions.

3. To the extent that the constitutional complaint challenges § 95.3 and 95.4 of the Telecommunications Act of 22 June 2004 (Federal Law Gazette I page 1190), it is dismissed as inadmissible.
4. Apart from this, the constitutional complaint is dismissed as unfounded.
5. The Federal Republic of Germany is ordered to reimburse the complainants one-third of their necessary expenses in the constitutional complaint proceedings.

### **Grounds:**

#### **A.**

The essential subject matter of the constitutional complaint is the constitutionality of §§ 111 to 113 of the Telecommunications Act. 1

#### **I.**

The complainants, as users of modern means of telecommunications, directly challenge §§ 111 to 113 TKG. On a judicious interpretation of their submissions, their challenges are directed more precisely against § 111.1, 111.2 and 111.4, § 112.1 to 112.4 and § 113.1 TKG, against the last also in conjunction with § 95.1 TKG. In addition, the complainants also specifically challenge § 95.3 and 95.4 TKG. 2

Originally, the constitutional complaint related to the version of the Telecommunications Act (Federal Law Gazette I p. 1190) which entered into effect on 26 June 2004. Later, the complainants extended their challenges to the amended versions of §§ 111, 112 TKG, which the provisions underwent in the year 2005 and in particular as a result of the Amendment Act (*Änderungsgesetz*) of 21 December 2007 (Federal Law Gazette I p.3198), which entered into effect on 1 January 2008. There were further amendments, which selectively extend the provisions but leave them unchanged in substance; however, the complainants did not include these in their constitutional complaint. The version of the Telecommunications Act on which the following is based and which is quoted from in the following is therefore based on the version in force on 1 January 2008. 3

1. a) § 111 TKG imposes a duty on commercial providers of telecommunications services to collect and store the telephone numbers, line identification numbers, mobile end device numbers and identifiers of email accounts (hereinafter collectively referred to as telecommunications numbers) which they allocate or provide and the related personal data of the subscribers such as names, addresses and dates of birth, also including the data of the commencement of contract; with regard to the email account identifiers, no independent duty of collection is imposed, but merely a duty of storage if it happens that these data are collected in any case. The provision is intended to provide a data basis for the information procedures governed by §§ 112 and 113 TKG.

4

b) § 112 TKG creates an automated procedure to give information from the data stored under § 111 TKG. According to this, providers of telecommunications services for the public must supply the data covered by § 111 TKG, in compliance with a statutory instrument which deals with the technical details (see § 112.3 TKG) in such a way that they can be retrieved by the Federal Network Agency (*Bundesnetzagentur*) without the knowledge of the providers (§ 112.1 TKG). In this connection, the possibility must be guaranteed of data retrieval using incomplete search data or a search with a similarity function. At the request of authorities described in more detail, the Federal Network Agency is to retrieve these data sets in the automated procedure and to transmit them to those authorities (see § 112.4 TKG). The authorities entitled include in particular the criminal prosecution authorities, the federal and *Land* (state) law enforcement authorities for purposes of warding off danger, the Central Office of the German Customs Investigation Service (*Zollkriminalamt*), the federal and *Land* authorities for the protection of the Constitution, the Military Counterintelligence Service (*Militärischer Abschirmdienst*) and the Federal Intelligence Service (*Bundesnachrichtendienst*), public safety answering points, the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*) and customs administration authorities for the purpose of combating undeclared work (see § 112.2 TKG). The information is supplied at all times insofar as it is necessary to discharge the statutory duties and the requests to the Federal Network Agency are made under the automated procedure (see end of § 112.2 TKG). The requesting authorities are responsible for the permissibility of the transmission; the Federal Network Agency only reviews these if there is a particular occasion (see § 112.4 sentence 2 and 112.3 TKG).

5

The statutory instrument provided for in § 112.3 sentence 1 TKG and the Technical Regulations (*Technische Richtlinie*) under § 112.3 sentence 3 TKG based on this have not yet been issued. However, under the transitional provision of § 150.12 sentence 3 TKG, the technical regulations are replaced by the interface description on the basis of § 90.2 and 90.6 of the Telecommunications Act of 25 July 1996 (*Telekommunikationsgesetz 1996* – TKG 1996, Federal Law Gazette I p. 1120) as long as the Technical Regulations have not been issued. According to information from the Federal Network Agency, at present the supply of information on data in the

6

automated procedure is not yet based on this interface description.

c) A manual procedure for information from the data stored under § 111 TKG is contained in § 113 TKG. In contrast to the automated information procedure, this provides for a duty of the telecommunications enterprises themselves to supply information. In the same way as in the automated information procedure, secrecy must be preserved on the supply of the information towards the persons to whom the data relate (see § 113.1 sentence 4 TKG).

7

In this connection, not only the suppliers who offer telecommunications services for the public have a duty of information, but all those who commercially provide telecommunications services or are involved in this (see § 113.1 in conjunction with § 3 no. 10 TKG). This also includes suppliers who provide data in authorities or enterprises, for example in hospitals and hotels, what are known as corporate networks or WLAN networks. The literature – on the basis of the figures stated in the legislature’s statement of intention on § 112 TKG 2004 (*Bundestag printed paper – Bundestagdrucksache – BTDrucks 15/2316, p. 95*) – proceeds on the assumption that § 113 TKG may affect up to 400,000 suppliers, whereas § 112 may at maximum affect several hundred persons subject to a duty (see Bock, in: Geppert/Piepenbrock/Schütz/Schuster, *Beck’scher Kommentar zum TKG*, 3rd ed. 2006, § 112, marginal no. 5).

8

The number of authorities entitled to receive information is also larger than in § 112 TKG. § 113.1 sentence 1 TKG contains no exhaustive listing of the authorities entitled to receive information with regard to general information, but defines the entitlement to information in abstract and task-related terms, and thus without restrictions for all authorities. Information is to be generally permissible insofar as this is necessary in the individual case to prosecute criminal offences and regulatory offences, to ward off dangers and to perform intelligence tasks.

9

The scope of the data covered by the duty of information also extends beyond § 112 TKG. In addition to the data covered by § 111 TKG, the duty of information here also extends to the data which the suppliers may collect and store for the purpose of substantively structuring, amending or terminating their contractual relationships under § 95.1 in conjunction with § 3 no. 3 TKG. Initially, in practice, these data are normally largely the same data as those covered by § 111 TKG, but they extend beyond these in that they may contain bank account details or personal information associated with special rates of payment.

10

In addition to the general duty of information of § 113.1 sentence 1 TKG, § 113.1 sentence 2 TKG contains a special duty of information with regard to data which serve to give protection against unauthorised access to end user devices or storage devices, such as in particular personal identification numbers (PINs) and numbers referred to as personal unblocking keys (PUKs). In this connection, those entitled to receive information include the criminal prosecution and security authorities and the intelligence services, in compliance with particular legal bases set out in § 113.1 sentence 2 TKG which contain general authorisations to collect data. The use of this

11

information to access data which are subject to the secrecy of telecommunications is permissible only under the requirements of the statutory provisions (see § 113.1 sentence 3 TKG).

d) The wording of §§ 111 to 113 TKG follows earlier provisions in the Telecommunications Act 1996. Even § 90 TKG 1996 imposed an obligation on telecommunications enterprises to keep customer databases which could be retrieved in an automated information procedure. In the same way, § 89.6 TKG 1996 imposed a duty on the service providers in a similar scope to that in § 113.1 sentence 1 TKG to supply information to state agencies in an individual case. According to a judgment of the Federal Administrative Court (*Bundesverwaltungsgericht*) of 22 October 2003 (Decisions of the Federal Administrative Court (*Entscheidungen des Bundesverwaltungsgerichts* – BVerwGE) 119, 123), however, § 90.1 TKG 1996 contained no duty to *collect* the customer data, but related solely to data which were permissibly collected in any case by the service providers in their own interest. This was of particular importance for what are known as prepaid products, in the case of which – for example in mobile communications – the customer acquires a credit balance in advance, which may then be spent by the use of telecommunications services. Depending on the structure of the services and contractual arrangements, it was possible in this way that telecommunications enterprises did not need to know the identity of their customers and in this way telecommunications services could be used anonymously and without the possibility of attributing them to subscribers. The reform of the law is intended to counteract this by the obligation to collect and store data under § 111 TKG.

12

e) The complainants additionally specifically challenge § 95.3 TKG, which they regard as inadequate; it provides that when the contractual relationship comes to an end, the data stored under § 95.1 TKG are to be deleted at the end of the following calendar year. They also challenge § 95.4 TKG, which entitles the service providers to require their customers to submit an official identification document and to make a copy of this, which is later to be destroyed.

13

2. The provisions which are at the centre of the challenges read as follows in the relevant version of 21 December 2007, which entered into force on 1 January 2008 and whose §§ 111 and 113.1 TKG continue in application today:

14

#### § 111 TKG

15

(1) A person who commercially provides telecommunications services or is involved in this and in the process issues telephone numbers or other line identification numbers or provides telecommunications connections for telephone numbers issued by others or other line identification numbers shall, for the information procedure under §§ 112 and 113, before activation collect and without undue delay store, even where these data are not necessary for operational purposes,

16

1. the telephone numbers and other line identification numbers,

17

2. the name and the address of the subscriber,

18

- 3. in the case of natural persons, their date of birth, 19
- 4. in the case of fixed-network connections, also the address of the line, 20
- 5. in cases in which both a mobile telephone connection and a mobile end user device are provided, the device number of this device and 21
- 6. the date when the contract commences; 22

when the date of the end of the contract is known, it shall also be stored. Sentence 1 also applies where the data are not entered in subscriber directories (§ 104). The duty of storage without undue delay under sentence 1 applies with regard to the data under sentence 1 nos. 1 and 2, with the necessary modifications, to a person which commercially provides a publicly accessible email service and in doing so collects data under sentence 1 nos. 1 and 2; in this case, the data under sentence 1 no. 1 shall be replaced by the identifiers of the email accounts and the subscriber under sentence 1 no. 2 shall be replaced by the owner of the email account. If the person subject to a duty under sentence 1 or sentence 3 obtains knowledge of a change, that person must correct the data without undue delay; in this connection, the person subject to a duty under sentence 1 must collect and store data not yet previously collected, insofar as it is able to collect the data without particular effort. The form of data storage for the information procedure under § 113 is optional. 23

(2) If the service provider under subsection 1 sentence 1 or sentence 3 uses a sales partner, the sales partner must collect the data under subsection 1 sentences 1 and 3 subject to the requirements set out there, and must transmit these data and the data collected under § 95 to the service provider without undue delay; subsection 1 sentence 2 applies with the necessary modifications. Sentence 1 also applies to data on changes insofar as the sales partner obtains knowledge of them in the ordinary course of business. 24

... 25

(4) The data shall be deleted at the end of the calendar year following the end of the contractual relationship. 26

... 27

### § 112 TKG 28

(1) A person who provides telecommunications services for the public shall without undue delay store the data collected under § 111.1 sentences 1, 3 and 4 and 111.2 in customer databases in which the following must also be entered: telephone numbers and sets of telephone numbers which are given to other providers of telecommunications services for further marketing or other use, and in the case of ported telephone numbers the current identifier. The correction and deletion of the data stored in the customer databases is governed by § 111.1 sentences 4 and § 111.4 with the necessary modifications. In cases of ported telephone numbers, the telephone number and the related identifier shall be deleted only after the end of the 29

year following the date on which the telephone number was re-assigned to the network operator to which it was originally allocated. The person subject to a duty shall ensure that

1. the Federal Network Agency, for requests for information from the agencies named in § 111.2, may at all times retrieve information from the customer databases within Germany using the automated procedure, 30

2. the retrieval of data is possible using incomplete search data or a search with a similarity function. 31

The requesting agency shall without undue delay review how far it needs the data which are supplied in response, and shall without undue delay delete data not needed. The person subject to a duty shall ensure by means of technical and organisational measures that it cannot obtain knowledge of retrievals. 32

(2) Information from the customer databases under § 112.1 shall under § 112.4 at all times be supplied to 33

1. the courts and criminal prosecution authorities, 34

2. the federal and *Land* (state) law enforcement authorities for purposes of warding off danger, 35

3. the Central Office of the German Customs Investigation Service (*Zollkriminalamt*) and the Customs Investigation Offices (*Zollfahndungsämter*) for the purposes of criminal proceedings, and the Central Office of the German Customs Investigation Service to prepare and carry out measures under § 39 of the Foreign Trade and Payments Act (*Außenwirtschaftsgesetz*), 36

4. the federal and *Land* authorities for the protection of the Constitution, the Military Counterintelligence Service, the Federal Intelligence Service, 37

5. the public safety answering points under § 108 and the answering point for the telephone number 124 124, 38

6. the Federal Financial Supervisory Authority and 39

7. the customs administration authorities for the purposes of combating undeclared work set out in § 2.1 of the Act to Combat Undeclared Work (*Schwarzarbeitsbekämpfungsgesetz*) 40

insofar as the information is necessary to discharge their statutory duties and the requests to the Federal Network Agency are submitted under the automated procedure. 41

(3) The Federal Ministry of Economics and Technology is authorised, by mutual agreement with the Federal Chancellery, the Federal Ministry of the Interior, the Federal Ministry of Justice, the Federal Ministry of Finance and the Federal Ministry of Defence, to issue a statutory instrument with the consent of the *Bundesrat*, laying 42



down

1. the essential requirements of the technical procedures 43
  - a) for the transmission of the requests to the Federal Network Agency, 44
  - b) for the retrieval of the data by the Federal Network Agency from the persons subject to a duty, including the types of data to be used for the search and 45
  - c) for the transmission of the results of the retrieval by the Federal Network Agency to the requesting agencies, 46
2. the security requirements to be complied with and 47
3. for retrievals using incomplete search data and for a search with a similarity function 48
  - a) the minimum requirements of the scope of the data to be entered, for the most precise determination of the person sought, 49
  - b) the characters which may be used in the search, 50
  - c) requirements for the use of linguistic procedures which guarantee that different spellings of the name of a person, a street or a place and deviations arising from the transposition, omission or addition of parts of names are included in the search and the search result, 51
  - d) the permissible amount of response data sets to be transmitted to the Federal Network Agency. 52

Apart from this, the statutory instrument may also provide for the possibility of search for the agencies named in §112.2 nos. 5 to 7 to be restricted to the scope necessary for these agencies. The technical details of the automated retrieval procedure shall be laid down by the Federal Network Agency in Technical Regulations to be prepared with the participation of the associations affected and the entitled agencies; as needed, this shall be adjusted to the state of the art and be published by the Federal Network Agency in its gazette. The person subject to a duty under § 112.1 and the entitled agencies shall satisfy the requirements of the Technical Regulations at the latest one year after they are promulgated. In the case of an amendment of the Technical Regulations, technical installations free of defects made in accordance with these regulations must at the latest three years after an amendment of these regulations enters into effect satisfy the amended requirements. 53

(4) At the request of the agencies named in § 112.2, the Federal Network Agency shall retrieve the relevant data sets from the customer databases under § 112.1 and transmit them to the requesting agency. It shall examine the permissibility of the transmission only where there is a particular occasion for this. The responsibility for the permissibility of the transmission shall be borne by the agencies named in § 112.2. For the purpose of data protection review by the agency responsible in 54

each case, the regulatory authority shall, for every retrieval, log the time, the data used in carrying out the retrieval, the data retrieved, a data item which unmistakably identifies the person retrieving and the requesting agency, its file reference and a data item which unmistakably identifies the person requesting. It is impermissible to use the log data for other purposes. The log data shall be deleted after one year.

...

55

#### § 113 TKG

56

(1) A person who commercially provides telecommunications services or is involved in this shall in the individual case supply to the competent agencies on their demand information on the data collected under §§ 95 and 111 insofar as this is necessary to prosecute criminal offences or regulatory offences, to ward off dangers to public security or order or to perform the statutory duties of the federal and *Land* authorities for the protection of the Constitution, the Federal Intelligence Service or the Military Counterintelligence Service. The person subject to a duty under sentence 1 shall, on the basis of a request for information under § 161.1 sentence 1, § 163.1 of the Code of Criminal Procedure (*Strafprozessordnung* – StPO), the data collection provisions of the federal or *Land* police statutes to ward off dangers to public security or order, § 8.1 of the Federal Act on the Protection of the Constitution (*Bundesverfassungsschutzgesetz*), the corresponding provisions of the *Land* statutes for the protection of the constitution, § 2.1 of the Federal Intelligence Service Act (*Bundesnachrichtendienstgesetz*) or § 4.1 of the Act on the Military Counterintelligence Service (*Gesetz über den militärischen Abschirmdienst* – MADG) supply information on data by means of which the access to end user devices or to storage devices used in these or in the network is protected, in particular PINs or PUKs; 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 permissible only subject to the requirements of the relevant statutory provisions. The person subject to a duty must preserve secrecy towards its customers and towards third parties with regard to the supply of information.

57

...

58

#### § 95 TKG

59

(1) The service provider may collect and use subscriber data insofar as this is necessary to achieve the purpose set out in § 3 no. 3. In connection with a contractual relationship with another service provider, the service provider may collect and use subscriber data of its subscribers and of the subscribers of the other service provider insofar as this is necessary to perform the contract between the service providers. The customer data shall be transmitted to third parties, unless this Part or another statute permits it, only with the subscriber's consent.

60

...

61

3. In practice, doubts have arisen in the use of § 113 TKG, and these have also concerned the non-constitutional courts. It is in particular at issue whether the provision also covers information on the owner of what is known as a dynamic internet protocol address (dynamic IP address). 62

The IP address is a number which makes it possible to contact computers and other technical devices in a network, in particular in the internet; in simple terms, it may be described as the computer's "telephone number". A distinction is made between static and dynamic IP addresses. Whereas a static IP address is firmly allocated to a particular subscriber (or more precisely to the network interface of a particular device of the subscriber), in the case of a dynamic address the subscriber (or more precisely the network interface of the device of the subscriber which communicates with the internet) is allocated a new IP address each time the device connects to the internet. The reason for this procedure is the scarcity of numbers available in the version of the internet protocol currently mainly in use. The dynamic addressing procedure is used in particular by suppliers of services which offer dial-up internet connections. At present, therefore, the general rule is that dynamic internet addresses are allocated for private internet use. However, current developments indicate that in future, on the basis of a new version of the internet protocol (Internet Protocol version 6) it will be possible to allocate addresses in the form of static IP addresses to a substantially greater extent. 63

It is undecided whether information may be requested under § 113 TKG as to which subscriber (or more precisely which network interface that can be attributed to a particular subscriber) was allocated a specific dynamic IP address – of necessity known to the retrieving authority – at a particular time. This is unclear because on the one hand the only subject of the information is the allocation of the requested number to a person and therefore what is known as customer data (see § 95.1 in conjunction with § 3 no. 3 TKG; admittedly, the term only applies to § 111 TKG in a sense going beyond the statutory definition), but on the other hand this information is only possible if the telecommunications enterprises first analyse the traffic data stored under § 96 TKG for this purpose and establish what connection the number in question was allocated to at the time in question; at the same time, this means that their information necessarily always relates to a specific connection. In the discussion on this, significance is attached to the equally contentious question as to whether the identification of a dynamic IP address is solely an encroachment upon Article 2.1 in conjunction with Article 1.1 of the Basic Law or at the same time an encroachment upon Article 10.1 of the Basic Law. There has not yet been a decision of the Federal Court of Justice (*Bundesgerichtshof*) on this issue. According to what is probably now the predominant view in case-law and literature, dynamic IP addresses may be retrieved by way of § 113 TKG (for example Münster Higher Administrative Court (*Oberverwaltungsgericht* – OVG), Order of 17 February 2009 – 13 B 33/09 –, *MultiMedia und Recht* (MMR) 2009, p.424; Zweibrücken Higher Regional Court (*Oberlandesgericht* – OLG), Order of 26 September 2008 – 4 W 62/08 –, MMR 2009, pp. 45-46; Graulich, 64

in: Arndt/Fetzer/Scherer, TKG, 2008, § 113, marginal no. 6; Kleszczewski, in: Säcker, *Berliner Kommentar zum TKG*, 2nd ed. 2009, § 113, marginal no. 6). The contrary view sees this as impermissible and permits information on it to be given only subject to strict requirements, such as under § 100 of the Code of Criminal Procedure; Karlsruhe Higher Regional Court, judgment of 4 December 2008 – 4 U 86/07 –, *Computer und Recht* (CR) 2009, pp. 373-374; Abdallah/Gercke, *Zeitschrift für Urheber- und Medienrecht* (ZUM) 2005, p.368 <373-374>; Bär, MMR 2005, pp. 626-627; Warg, MMR 2006, p. 77 <81>).

## II.

The complainants use prepaid mobile phone cards and internet access services of more than one supplier. They are of the opinion that their fundamental rights under Article 10.1, Article 2.1 in conjunction with Article 1.1 and under Article 3.1 of the Basic Law are violated by the challenged provisions. 65

They assert as follows: that it is relatively probable that they are affected by searches under §§ 112 and 113 TKG for data stored on themselves. They submit that it is not improbable that persons who they know might be involved in investigation proceedings and in the course of these the complainants' telephone numbers might be examined. They would have no knowledge of search under §§ 112 and 113 TKG. They submit that they cannot reasonably be expected to obtain information from all authorities entitled under these provisions to search, particularly since, although non-constitutional law gives rights of information with regard to stored data, it does not do so in relation to the retrieval of data carried out in the past. 66

They submit that 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 referred to as Directive 2006/24/EC) does not make the constitutional complaint inadmissible. It does not mandatorily lay down the challenged provisions; apart from this, there are also doubts as to the lawfulness of the Directive. It was issued *ultra vires* and violates human rights to respect for private life and correspondence under Article 8 of the European Convention on Human Rights (ECHR) and freedom of expression under Article 10.1 ECHR. Even if one accepts that there is a duty of implementation, they submit, the constitutional complaint is admissible in order to enable reference to the Court of Justice of the European Union (CJEU) by the Federal Constitutional Court to clarify whether it is valid. 67

In the view of the complainants, the storage of telecommunications customer data provided for in § 111 TKG and the possibilities of retrieval provided for in §§ 112 and 113 TKG violate Article 10.1 of the Basic Law. The secrecy of telecommunications also includes the collection and use of telecommunications customer data. Customer data describe the individual communications events in more detail in that they provide information on whether a communication medium was used and, if so, provide further 68

communications-related information. The information on the owners of telephone numbers reveals which persons communicated with each other. Article 10.1 of the Basic Law guarantees that confidential telecommunication is possible. However, this requires that it is possible for telecommunication to occur anonymously and that the subscribers are protected against being identified. Customer data too must, as data on the identity of telecommunications subscribers, be subject to the secrecy of telecommunications.

The complainants further submit that the provisions of §§ 111 to 113 TKG procedurally violate the citation requirement of Article 19.1 sentence 2 of the Basic Law. Substantively, they are disproportionate. The provisions of §§ 111 to 113 TKG are not comparable to the storage and transmission of other data, such as main account data, residents' registration data and data from the motor vehicle registers. The provision of § 113 TKG is relevant in practice above all in pursuing copyright violations in the internet by way of dynamic IP addresses.

69

The complainants emphasise above all that § 111 TKG introduces a duty to collect and store personal data for retention; this duty violates the prohibition of data retention for purposes that are indefinite or cannot yet be determined. General descriptions of duties such as purposes of criminal prosecution or purposes of warding off danger are not an adequate intended purpose in this sense. The provision creates a system of precautionary state surveillance which is unique to date. At the same time, the provision dispenses with every degree of suspicion and with every proximity to danger of the persons affected. It is disproportionate to prohibit the possibility of anonymous communication for the whole population despite the fact that this possibility is only abused by a few. If people were to abstain from communication with others out of fear of disadvantages, this would inflict harm on a democratic society. At all events, the serious encroachment upon fundamental rights created by § 111 TKG is disproportionate. A systematic storage of customer data is scarcely qualified to encourage general interests. Criminals often use telecommunications services anonymously or using a false name, and therefore the storage of customer data cannot contribute a great deal to the successful investigation of crimes. Even without § 111 TKG, effective criminal prosecution and effective exercise of other state duties are possible. In contrast, a systematic storage of data is an extremely intensive encroachment, because it makes it possible to reproduce telecommunications behaviour at all times. It is mistaken to attribute less sensitivity to customer data than to traffic data and the contents of communications, since customer data and telecommunications contents are only informative in combination with each other.

70

§§ 112 and 113 TKG create not only a duty of information for the service providers, but also an entitlement to collect data of the authorities entitled to receive information, without an additional authorising provision being necessary. Apart from this, a general data collection authorisation under non-constitutional law is not sufficient to give authorisation for the transmission of personal data. On the contrary, this requires an authorisation of transmission with well-defined provisions. §§ 112 and 113 TKG, ac-

71

ording to the legislature's intention, permit individual communication events to be attributed to the person participating in the communication. There must be uniform thresholds of encroachment for the access to information on telecommunications and its participants. The distinction according to customer data, traffic data and content data is irrelevant to the definition of this.

§§ 112 and 113 TKG are disproportionate because the requirement for transmission that it should be necessary to perform the tasks of the retrieving authority is completely inadequate as a restrictive element. Retrievals of customer data can only be proportionate if they are intended to prosecute serious offences. But neither §§ 112 and 113 TKG nor the non-constitutional law applying to the retrieving authorities lay down a limitation of use to specific purposes which corresponds to the severity of the encroachment upon fundamental rights. §§ 112 and 113 TKG also violate the requirement that legislation should be definite and clear, since, measured against the intensity of the encroachment, they insufficiently legislate on the extent of authorisation to encroach. The provisions which permit intensive encroachment do not define the purposes with sufficient precision, and nor does § 113 TKG define the target group of the data retrieval with sufficient precision.

72

Especially a search with incomplete data or wildcards results in a very large number of search results and is very invasive. There will be confusions of names and investigation measures against persons who merely have a similar name, although the persons affected have not given any occasion for this. § 113.1 sentence 2 TKG, which permits a search in sensitive access data with an increased need for protection, also fails to take adequate account of the weight of the encroachments upon fundamental rights made possible by these data.

73

§ 95.3 TKG also violates Article 10.1 of the Basic Law. Telecommunications enterprises are subjected to a duty to store customer data for longer than is necessary for their purposes. At the same time, rights of access are given to state authorities.

74

Finally, the principle of equality before the law is violated, since the use of telecommunications is disadvantaged, without objective justification, in contrast to other forms of distance communication and to communication in immediate spatial vicinity.

75

### III.

Opinions on the constitutional complaint were submitted by the Federal Government, the Federal Administrative Court, the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*), the Commissioner for Data Protection and the Right to Inspection of Files for the *Land Brandenburg (Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht)* and the Berlin Commissioner for Data Protection and Freedom of Information (*Beauftragter für Datenschutz und Informationsfreiheit*).

76

1. The Federal Government is of the opinion that the constitutional complaint is at least in part inadmissible, and that in other respects it is at all events unfounded.

77

a) On a point of fact, the Federal Government submits as follows: In practice, the automated retrieval procedure under § 112 TKG is of primary importance. Experience has shown that the number of retrievals in the procedure under § 113.1 TKG is between 3% and 5% of the number of requests under § 112 TKG. The automated retrieval procedure is used primarily for purposes of the prosecution of criminal offences. The number of retrievals for warding off danger or for intelligence purposes is insignificant. 78

In the practice of criminal prosecution, retrievals under §§ 112 and 113 TKG are used above all in three typical fact situations: in the first situation, which comprises approximately two-thirds of the cases, the retrievals are not connected to measures of telecommunications surveillance but serve to connect a telephone number which becomes known in investigation proceedings to a person, for example when notes are seized and these contain unknown telephone numbers. In the second, less common group of cases, a retrieval prepares for a measure of telecommunications surveillance by investigating what telephone numbers and connections are owned by the person to be observed. In the third group of cases, telecommunications surveillance is followed up by determination of the owners of telephone numbers which became known during such a procedure. In total, approximately 95% of the retrievals relate to the determination of the person behind a known telephone number. 79

In recent years, the number of retrievals of customer data has continuously increased. At the beginning of the 1990s, there were approximately 350,000 to 500,000 retrievals of customer data per year from the German Administration of Posts and Telecommunications (*Deutsche Bundespost*), as it then was. In recent years, the number of automated retrievals per year has risen from 1.5 m in the year 2001 to 3.4 m in the year 2005. The increase results primarily from the changed telecommunications behaviour of the population and in particular from the groups of persons relevant for the security authorities. The number of authorities and telecommunications enterprises taking part in the automated information procedure under § 112 TKG has also further increased. At the end of 2009, approximately 1,000 authorities registered with the Federal Network Agency could have retrieved data from 120 telecommunications enterprises. In the year 2008, 4.2 m requests from security authorities resulted in 26.6 m retrievals from the telecommunications enterprises (Federal Network Agency, *Tätigkeitsbericht 2008/2009 Telekommunikation*, p. 245). 80

b) There are doubts as to whether the constitutional complaint is even admissible. From a legal point of view it is doubtful whether the complainants are personally, presently and directly affected by the provisions of §§ 112, 113 TKG. They did not show that there was some probability that they would be affected by a retrieval of customer data. With regard to the requests for information using incomplete search data or using a similarity function under § 112.1 sentence 4 TKG, the complainants are not presently affected, because the statutory instrument and Technical Regulations to be issued under § 112.3 TKG do not yet exist. The fundamental decision to store the essential customer data for retention is mandatorily laid down by the European Data 81

Retention Directive. Even if the duty of storage goes beyond § 111 TKG, this excludes a review under the standard of the Basic Law. In addition, the complainants may challenge the duty of collection and storage in proceedings against the service provider, and consequently the subsidiarity of the constitutional complaint is not guaranteed. With regard to § 95.3 TKG, the constitutional complaint is inadmissible because the provision does not contain a duty to store data, but only a right to do so.

c) The challenged provisions are to be measured not against Article 10.1 of the Basic Law, but against the right to informational self-determination. Article 10.1 of the Basic Law protects the confidentiality of the contents of communication and of the specific circumstances of communications events. The customer data in question have no connection to this, for it is impossible to make inferences from them with regard to the circumstances or contents of specific conversations. Nor is the retrieval of access data under § 113.1 sentence 2 TKG an encroachment upon Article 10.1 of the Basic Law. At most, these data may make it possible to have subsequent access to traffic data; but merely collecting the access data is not access to the traffic data themselves.

82

d) The encroachment upon the right to informational self-determination constituted by information on customer data is not solely attributable to §§ 112, 113 TKG. The security authorities which request information act in each case on the basis of a non-constitutional statute which applies to them, for example a police statute or the Code of Criminal Procedure, which always requires suspicion of a criminal offence as the threshold of encroachment for criminal investigation proceedings. §§ 112, 113 TKG were not intended to remove the complex provisions of the non-constitutional statute and replace them by a definitive uniform provision which applies to all security authorities. On the contrary, these provisions were conceived in order to interact with the non-constitutional law applicable in each case; this non-constitutional law alone is capable of supplying the actual authorisation to collect the personal data. In addition to this, §§ 112, 113 TKG create the requirements under telecommunications law for an authority actually to receive the information which it is entitled to collect, by providing for a duty of the telecommunications enterprises to make data available and to give information and for a retrieval procedure.

83

e) Admittedly, the duty of collection and storage laid down in § 111 TKG encroaches upon the general right of personality of telecommunications customers, but this encroachment is not very strong. With the exception of prepaid products, the telecommunications enterprises already store the data in question in their own interest. The data collected, as basic data to determine how a person can be contacted by telecommunications, are not highly sensitive and are comparable to the data on residence or motor vehicles which have long been stored in public registers. The encroachment caused by § 111 TKG is not of particular weight for the mere reason that it makes anonymous telephoning impossible. The interest in anonymity does not enjoy protection over and above the general protection of fundamental rights. The duty of storage of § 111 TKG is suitable and necessary to achieve its objectives. The sys-

84



tematic collection of telephone customer data is of indispensable added value for the security authorities in contrast to access to other data sets. It is also proportionate in the narrow sense. Its unquestionable benefit stands against an encroachment which has little weight. Finally, § 111 TKG does not provide for an impermissible data retention, for the provision defines the purpose with sufficient clarity in referring to public security.

The statutory amendments referred to by the complainants extend the duties of collection and storage to other line identification numbers in order to react to the fact that today the stored telephone numbers alone are insufficient to guarantee that the subscriber data can be determined, for example because other identifiers are also issued in DSL technology. In this way, the collection of customer data is extended to include a new phenomenon, without acquiring a new quality. The duty to store the device numbers of mobile telephones is also only a reaction to a de facto phenomenon which threatens to defeat the purpose of the information on customer data. For if persons charged with an offence use more than one mobile phone card for only one mobile phone, information relating to the line is no longer sufficient. The storage of customer data in connection with email services serves to implement Directive 2006/24/EC. It takes account of the fact that the identifier of an email account has now become a fundamental identification feature of accessibility in telecommunications, comparable to telephone number and address.

85

f) § 112 TKG is also in conformity with the Basic Law. The encroachment upon the right to informational self-determination constituted by automated information on telecommunications customer data may be attributed to § 112 TKG only to a limited degree, since the legal relationship between the security authority and telecommunications customers is shaped by the non-constitutional law which contains the authorising provisions for data collection. The only duty of § 112 TKG is to support the non-constitutional authorising provision with a retrieval procedure and a duty to make data available, but not to formulate the relevant threshold of encroachment. In addition, § 112.2 TKG defines the criterion of necessity, as an additional condition for encroachment. The encroachment is insignificant, since it affects basic identification data with a low degree of personal relevance and a high degree of social reference. For this reason, the secrecy of the retrieval does not have the same weight as in other combinations of circumstances. The question as to how far the person affected is to be informed of retrievals of customer data or how far the person affected has a right of information, on the other hand, is to be answered by non-constitutional law. In addition, in mass procedures in the case of insignificant encroachments there is no constitutional duty of notification. The subsequent use of the data obtained under § 112 is based on the relevant non-constitutional law of the requesting authorities, which contains corresponding limitations to specific purposes.

86

The possibility contained in § 112.1 sentence 4, 112.3 TKG of using incomplete search data or a search with a similarity function is unobjectionable. Admittedly, the search may have a certain range, but the encroachment even here is insignificant,

87

since it relates only to identification data. The search is unsuited to electronic profile searching. In police law, informational encroachments may not be directed only against persons endangering public security or order and in criminal procedure too it is not unusual for outsiders. The criterion of necessity takes account of proportionality. In permitting a linguistic procedure, the amended law pursues the objective of implementing searches with the help of a similarity function in an effective manner. This is not a qualitatively novel instrument of investigation.

g) § 113 TKG also remains within the scope of the legislature's assessment that the security authorities should be supplied with telecommunications customer data for their purposes; this assessment is not disproportionate. It is unobjectionable that the group of agencies entitled to receive information in § 113.1 TKG is larger than that in § 112.2 TKG. The warding off of danger by the regulatory authorities and the prosecution of regulatory offences may also justify the encroachment. It is also unproblematic that under the manual information procedure enterprises which provide non-public services are among the agencies with a duty of information. Nor does the possibility of access to PINs and PUKs under § 113.1 sentence 2 TKG result in a particularly significant encroachment.

88

The possibility of access to other customer data stored under § 95 TKG for business purposes is also unobjectionable. Some of the identification information stored is not worthy of a higher degree of protection than the customer data to be stored under § 111 TKG; in the case of other contract data, the criterion of necessity may be applied more strictly. The weight of the encroachment is reduced by the fact that the only data which can be retrieved are those which a service provider has stored for its own purposes.

89

2. In its opinion, the Sixth Appeal Panel (*Revisionssenat*) of the Federal Administrative Court refers to its judgment of 22 October 2003 (BVerwGE 119, 123).

90

3. The Federal Commissioner for Data Protection and Freedom of Information regards the challenged provisions as an unconstitutional violation of the right to informational self-determination and submits as follows. The provision of § 111 TKG contains a disproportionate comprehensive duty of storage and violates the prohibition of a collection of data for retention for purposes that are indefinite or cannot yet be determined. Measured against the intended purpose of the information, the powers to supply information under § 112.2 TKG, are too comprehensive and indefinite. § 113 TKG is also disproportionate. The indefinite wording of the provision and the broad authority to encroach which it contains do not do justice to the high degree of protection required by the data affected. It is not comprehensible that the authority to access the access data of § 113.1 sentence 2 TKG is made available subject to such lenient conditions despite the fact that access to the content data behind them is subject to stricter conditions.

91

4. The Commissioner for Data Protection and the Right to Inspection of Files for the *Land* Brandenburg, who also expressed an opinion on behalf of twelve other *Land*

92

data protection officers, regards the challenged provisions, measured against the right to informational self-determination, as predominantly unconstitutional and submits as follows. The duty of storage of § 111 TKG violates the prohibition of data storage for retention; the provision is just as disproportionate as §§ 112, 113 TKG. The only situation when the provision of § 113 TKG does not encroach upon the area of protection of Article 10.1 of the Basic Law is if its area of application is not overstretched. The supply of information on the identity of an internet user when the dynamic IP address is known must be regarded as information on traffic data and thus is not permitted, on the basis of § 113 TKG,.

5. The Berlin Commissioner for Data Protection and Freedom of Information also regards the challenged provisions in their original wording as predominantly unconstitutional. Admittedly, he submits, § 95.3 TKG is not subject to objections under constitutional law, but § 111 TKG violates the right to informational self-determination. Unlike § 112.1 TKG, § 112.2 gives authority to encroach upon Article 10.1 of the Basic Law. The requirements for retrievals under § 112 TKG are drafted too indefinitely, and there is a lack of constitutional safeguards of informational self-determination.

93

## B.

The constitutional complaint is predominantly admissible.

94

## I.

1. However, the constitutional complaint is inadmissible insofar as it challenges a violation of Article 3.1 of the Basic Law. The complainants' submission when they regard it as unjustified unequal treatment that storage is laid down only for the exchange of information via telecommunications networks but not for exchange of information in immediate spatial vicinity or by post does not satisfy the substantiation requirements of § 23.1 sentence 2, § 92 of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz – BVerfGG*). In particular they do not sufficiently show to what extent the two groups which they have established for comparison represent essentially the same fact situation.

95

2. The constitutional complaint is also inadmissible insofar as the complainants challenge § 95.3 TKG and § 111.4 TKG. The interpretation of these provisions has not yet been resolved, in particular with regard to the question as to whether the time limit they lay down is a strict time limit or merely a maximum time limit which also permits earlier deletion where this may be constitutionally required (see Bock, in: *Gepfert/Piepenbrock/Schütz/Schuster, Beck'scher Kommentar zum TKG*, 3rd ed. 2006, § 111, marginal no. 14; Kleszczewski, in: *Säcker, Berliner Kommentar zum TKG*, 2nd ed. 2009, § 111, marginal no. 23; Reimann, *Datenschutz und Daten* 2004, p. 421 <424>). Since the complainants have the possibility, after their contracts with their service providers end, to have this question first resolved by the non-constitutional courts, it cannot be said that all legal remedies are exhausted in this respect (see § 90.2 sentence 1 BVerfGG).

96

Nor is the challenge to § 95.4 TKG admissible. Admittedly, the constitutional complaint expressly challenges this provision, but it does not deal factually with its contents, and it therefore fails to satisfy the requirements of § 23.1 sentence 2, § 92 BVerfGG. 97

Finally, the constitutional complaint is also inadmissible with regard to the power under § 112.3 TKG to issue a statutory instrument, which is *inter alia* to provide for the procedure and extent of a search with a similarity function. Since such a statutory instrument on the basis of § 112.3 TKG has not yet been issued, the complainants are not directly and presently affected by the provision. 98

## II.

Apart from this, the constitutional complaint is admissible. 99

1. The complainants admissibly challenge a violation of the right to informational self-determination under Article 2.1 in conjunction with Article 1.1 of the Basic Law and of the secrecy of telecommunications under Article 10.1 of the Basic Law. They use prepaid mobile phone cards and internet access services and submit that the storage of their data and the possibility that these are transmitted under the information procedure of §§ 112 and 113 TKG violate their fundamental right to informational self-determination and to preservation of the secrecy of telecommunications. Notwithstanding the question of the precise delimitation of these fundamental rights, it is at all events possible that one of the two fundamental rights of the complainants is violated by the challenged provisions. 100

2. The challenged provisions also affect the complainants directly, personally and presently. Admittedly, the duties to store data, make data available and supply information of §§ 111 to 113 TKG are not directed to the complainants, who are affected as users, but to the service providers or the Federal Network Agency. However, these have an absolute duty, without any latitude of decision, to store the complainants' data and to supply information. The challenged provisions therefore result directly and presently in the storage and use of the complainants' data (see Decisions of the Federal Constitutional Court (*Entscheidungen des Bundesverfassungsgerichts – BVerfGE*) 125, 260 <304-305>). 101

The fact that §§ 112 and 113 TKG only take effect on the basis of further acts of performance in the form of requests or demands for information and the subsequent supply of information does not mean that the complainants are not directly and personally affected. Since the complainants do not obtain knowledge of the acts of performance, the submissions are sufficient to show that there is some probability that they are affected by such measures. In this connection, it is particularly relevant that the information made possible by § 112.2 and § 113.1 TKG has a great range and may also include outsiders by chance. Submissions in which the complainants would be obliged to incriminate themselves are unnecessary to show that they are personally affected, and equally unnecessary is a submission that they are responsible for activities 102

which endanger security or are of relevance to intelligence (see BVerfGE 125, 260 <305>).

The constitutional complaint is not time-barred. It is true that there were already both an automated information procedure and a manual information procedure in the Telecommunications Act 1996. The provisions challenged in the present case, however, fundamentally restructure these information procedures and change their significance, in particular through their connection with a newly defined duty of data collection. The one-year period of § 93.3 BVerfGG therefore began to run again when this statute entered into force on 26 June 2004 (see BVerfGE 11, 351 <359-360>; 74, 69 <73>; 78, 350 <356>). The constitutional complaint received by the Federal Constitutional Court on 21 June 2005 is therefore within the time limit, as is the application received on 1 February 2008 to extend the constitutional complaint to include the amendments of §§ 111 and 112 TKG which entered into force on 1 January 2008. 103

3. The constitutional complaint is not inadmissible with regard to higher-ranking law of the European Union. 104

However, in principle the Federal Constitutional Court does not review domestic provisions which implement mandatory requirements of European Union law in German law against the standard of fundamental rights of the Basic Law; constitutional complainants directed against these are in general inadmissible (see BVerfGE 118, 79 <95>; 121, 1 <15>; 125, 260 <306>). In addition, the constitutional complaint, insofar as it challenges § 111.1, 111.2 TKG, challenges a provision which is essentially determined by European Union law. The extent of the duty of storage contained in § 111.1, 111.2 TKG and challenged by the complainants is likely – at least in essence – to be controlled under European Union law by Article 5 of Directive 2006/24 EC. 105

Nevertheless, the constitutional complaint is also admissible in this connection. The complainants – with submissions identical to those in the proceedings 1 BvR 256/08 and others, which the first complainant at times conducted in parallel and in relation to the same Directive (see BVerfGE 125, 260) – submit that the Directive named is invalid and seek a reference by the Federal Constitutional Court to the Court of Justice of the European Union, in order that the latter, in a preliminary ruling under Article 267 TFEU, declares the Directive null and void and thus opens the way for a review of the challenged provisions by the standard of German fundamental rights. In this way, it is not from the outset ruled out that the provisions challenged by them directly and without further possibilities of redress can be reviewed against the standard of the Basic Law (see BVerfGE 125, 260 <306-307>). With regard to European Union law, there are no doubts as to the admissibility of the challenges of § 112 and § 113 TKG among other reasons because the German legislature is not subject to any mandatory requirements of European Union law in drafting provisions on the use of data. These provisions are therefore to be reviewed without restriction against the standard of German fundamental rights. 106

### C.

The constitutional complaint is well-founded in part. 107

However, the constitutional complaint is unfounded insofar as the complainants challenge § 111 and § 112 TKG. The constitutional complaint is also unsuccessful insofar as it challenges § 113.1 sentence 1 TKG as such. § 113.1 sentence 1 TKG must, however, be interpreted in conformity with the Basic Law to the effect that no duty of information of the telecommunications service providers is created by it alone; on the contrary, there is a need for a retrieval provision of non-constitutional law, which must create an independent and clearly defined duty of the service providers. In addition, § 113.1 sentence 1 TKG must be constitutionally defined to the effect that the provision does not permit an attribution of dynamic IP addresses. Finally, the constitutional complaint is also well-founded insofar as it challenges § 113.1 sentence 2 TKG. 108

### I.

The central criterion is the right to informational self-determination under Article 2.1 in conjunction with Article 1.1 of the Basic Law. 109

1. The challenged provisions do not encroach upon the secrecy of telecommunications of Article 10.1 of the Basic Law. However, the situation is different with regard to § 113.1 TKG, insofar as this is understood as an authorisation for the attribution of dynamic IP addresses. 110

a) Article 10.1 of the Basic Law guarantees the secrecy of telecommunications, which protects the incorporeal transmission of information to individual recipients with the aid of telecommunications traffic against the taking of notice by state authority (see BVerfGE 125, 260 <309> with further references). This is intended to avoid the exchange of opinion and information by way of telecommunications installations ceasing or its form and content being changed because the parties must expect that government agencies will monitor the communication and obtain information on the communication relationships and communication content (see BVerfGE 100, 313 <359>; 107, 299 <313>). 111

aa) Article 10.1 of the Basic Law does not only cover the contents of communication. On the contrary, the protection also covers the confidentiality of the immediate circumstances of the communications event, 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>; 100, 313 <358>; 107, 299 <312-313>; 125, 260 <309>; established case-law). An encroachment upon Article 10.1 of the Basic Law is therefore also made, for example, if malicious caller identification is used and without the knowledge of the person telephoning a connection is established in such a way that the call can be traced back (see BVerfGE 85, 386 <395 ff.>) or calling line identification restriction is cancelled (see § 101 TKG). 112

However, Article 10.1 of the Basic Law solely protects the confidentiality of specific telecommunications events. But its protection does not extend generally to all information which relates to the telecommunications behaviour or the totality of relations between the telecommunications service providers and their customers. In particular, the secrecy of telecommunications does not protect the confidentiality of the circumstances of each provision of telecommunications services, such as for example the attribution of the telecommunications numbers allocated by the service providers to particular subscribers. 113

bb) Nor does the attribution of a telecommunications number to a subscriber affect Article 10.1 of the Basic Law even where it indirectly enables an authority to reconstruct the contents or the circumstances of specific communications events and to attribute them to a specific person. Admittedly, the attribution of a telephone number need not be restricted to the information as to which subscriber is behind a number, such as is the case, for example, if authorities investigate telephone numbers which they have received as the content of notes. On the contrary, such an attribution makes it indirectly possible to establish the individual details of the circumstances and content of a call, for example where the content and time of a particular call which was made from the retrieved number is known to the authority through preliminary investigations. However, neither does the possibility of obtaining such information content mean that the attribution of a telecommunications number to its subscriber is relevant in regard to Article 10.1 of the Basic Law. For in this case too, the information on content and circumstances of the act of telecommunications in question is not obtained by the encroachment upon confidential telecommunications events itself, but only transpires in connection with knowledge which the authority has obtained elsewhere, whether through its own investigations, whether from the statements of third parties, in particular, for example, from notice given by a party to telecommunications. Article 10.1 of the Basic Law protects the confidentiality of the use of the technical medium used for transmitting messages, but not the trust between the parties to communications. The secrecy of telecommunications gives no protection against the disclosure of the content or circumstances of an act of communication by a party to the communications (see BVerfGE 85, 386 <399>; 106, 28 <37>). On the contrary, the mere attribution of a telecommunications number to a subscriber leaves the confidentiality of the specific communications event as such unaffected and thus does not interfere with Article 10.1 of the Basic Law. 114

This applies to line identification numbers or identifiers of email accounts just as to telephone numbers. But exactly the same applies to static IP addresses. Admittedly, the attribution of a static IP address to a particular subscriber – more precisely, to a network interface of the subscriber – as a rule also gives indirect information on a particular telecommunications event involving the person in question, since such addresses, even if they are static, are registered and become the subject of attributions identifying an individual almost only in connection with specific communications events. However, here too the conveying of information in this connection is as such 115

limited exclusively to the abstract attribution of number and subscriber.

cc) In contrast, the situation is different when dynamic IP addresses are attributed to identified persons, for such addresses are particularly closely related to specific telecommunications events. This attribution is within the area of protection of Article 10.1 of the Basic Law. However, here too this does not automatically follow from the fact that the attribution of a dynamic IP address necessarily always relates to a specific telecommunications event of which it therefore indirectly also provides information. For in this connection too the information itself only relates to data which are abstractly attributed to a subscriber. There is therefore no fundamental difference from the attribution of static IP addresses. However, the application of Article 10.1 of the Basic Law is here based on the fact that when the telecommunications enterprises identify a dynamic IP address, they have to take an intermediate step, in which they examine the relevant connection data of their customers, that is, must access specific telecommunications events. These telecommunications connections individually stored by the service providers are subject to the secrecy of telecommunications, irrespective of whether they have to be kept available by the service providers under a statutory duty (see BVerfGE 125, 260 <312-313>) or whether they are stored by them on a contractual basis. Insofar as the legislature imposes a duty on the telecommunications enterprises to access these data and to evaluate them in the interest of the state's performance of its duties, this is an encroachment upon Article 10.1 of the Basic Law. This is the case not only if the service providers must supply the connection data themselves, but also if they have to use the data as a preliminary question for information.

116

b) In conclusion, § 111 and § 112 TKG do not affect the secrecy of telecommunications. In contrast, § 113.1 TKG encroaches upon Article 10.1 of the Basic Law to the extent that it is a basis for the supply of information on dynamic IP addresses. Apart from this, § 113.1 TKG too is not to be measured against Article 10.1 of the Basic Law.

117

The storage required in § 111.1, 111.2 TKG relates exclusively to the abstract attribution of numbers, line identification numbers and identifiers of email accounts to specific subscribers who are more closely identified. It therefore does not encroach upon Article 10.1 of the Basic Law. According to the above standards, this applies irrespective of whether, under non-constitutional law, the static IP addresses are also to be deemed to be line identification numbers under § 111.1 sentence 1 TKG. Under § 111.1, 111.2 TKG, specific communications connections are not subject to the duty of storage.

118

Similarly, information under §§ 112 and 113 TKG does not encroach upon the secrecy of telecommunications. For information with regard to the data stored under § 111 TKG, this is a clear consequence of the above remarks. But the same applies insofar as § 113.1 TKG in addition covers the data stored by the service providers under § 95.1 TKG. For the data known as customer data which are permissibly stored

119



by service providers under this provision (see § 3 no.3 TKG) give no information on specific telecommunications connections.

However, § 113.1 TKG does create an encroachment upon Article 10.1 of the Basic Law insofar as, in current practice, it is relied on to enable an attribution of dynamic IP addresses to their subscribers (see OVG Münster, Order of 17 February 2009 – 13 B 33/09 –, MMR 2009, p. 424; OLG Zweibrücken, Order of 26 September 2008 – 4 W 62/08 –, MMR 2009, pp. 45-46; Cologne Regional Court (*Landgericht* – LG), Order of 14 October 2008 – 106 Qs 24/08 –, CR 2008, p. 803 <804>). For insofar as the telecommunications enterprises have to supply information on this, they are initially obliged to access the traffic data stored by themselves under § 96 TKG and to evaluate them. However, since these data are subject to the protection of the secrecy of telecommunications, a government-imposed duty to use them is to be measured against Article 10.1 of the Basic Law. 120

2. The challenged provisions encroach upon the right to informational self-determination. 121

a) The right to informational self-determination takes account of endangerments and violations of personality which arise in the conditions of modern data processing from information-related measures (see BVerfGE 65, 1 <42>; 113, 29 <46>; 115, 166 <188>; 115, 320 <341-342>; 118, 168 <184>; 120, 378 <397>). The free development of personality presupposes the protection of the individual against unrestricted collection, storage, use and transmission of the individual's personal data. This protection is therefore covered by the fundamental right of Article 2.1 in conjunction with Article 1.1 of the Basic Law. In this respect, the fundamental right guarantees the authority of the individual in principle himself or herself to decide on the disclosure and use of his or her personal data (BVerfGE 65, 1 <43>; 113, 29 <46>). The guarantee of the fundamental right takes effect in particular when the development of personality is endangered by government authorities using and combining personal information in a manner which persons affected can neither fully appreciate nor control (see BVerfGE 118, 168 <184>). The extent of protection of the right to informational self-determination is not restricted to information which by its very nature is sensitive and for this reason alone is constitutionally protected. In view of the possibilities of processing and combining, there is no item of personal data which is in itself, that is, regardless of the context of its use, insignificant (see BVerfGE 65, 1 <45>; 118, 168 <185>; 120, 378 <398-399>; established case-law). In particular, the protection of informational self-determination also includes personal information on the procedure by which telecommunications services are provided. 122

Provisions which give authority for government authorities to deal with personal data as a rule create a number of encroachments which build on each other. In this respect, a distinction must in particular be made between the collection, storage and use of data (see BVerfGE 100, 313 <366-367>; 115, 320 <343-344>; 120, 378 <400-401>; 125, 260 <310>). In legislating for data exchange for the purpose of the 123

performance of government duties, however, a distinction must also be made between data transfer by the party supplying the information and data retrieval by the agency seeking the information. A data exchange takes place through the encroachments of retrieval and transfer, which correspond to each other and each of which requires an independent legal basis. Figuratively speaking, the legislature must open not only the door for the transmission of data, but also the door for their retrieval. It is only both legal bases together, which must operate together like a double door, which give authority to exchange personal data. This does not exclude – subject to the system of competencies and the requirements of clear drafting – the possibility of both legal bases being contained in one provision.

b) The challenged provisions encroach upon the complainants' fundamental right to informational self-determination. Firstly, there are encroachments upon the duty of collection and storage of § 111 TKG. There are independent further encroachments upon fundamental rights by the duty of service providers laid down in § 112.1 TKG to make the data available as customer databases which can be accessed in an automated procedure and by the authority of the Federal Network Agency to retrieve these data and to transmit them to particular authorities (see § 112.4 TKG). Accordingly, § 113.1 sentences 1 and 2 TKG create independent encroachments upon fundamental rights by imposing on the telecommunications service providers a duty to provide information on demand with regard to the data stored by themselves.

124

Finally, § 112 and § 113 TKG are subject to prior retrieval of the data by the authorities entitled to retrieve, in the form of a request (§ 112.1, 112.2, 112.4 TKG) or a demand (§ 113.1 TKG); this constitutes an independent encroachment which must be distinguished from the foregoing. But under the legislature's legislative concept, this also requires a further legal basis, which must be contained in federal or *Land* legislation, depending on the area involved. The provisions of §§ 112 and 113 TKG – corresponding to the distinction between collection and transmission in the legislative typology of the data protection Acts – are to be understood solely as the legal basis for the transmission. They presuppose that the authorities entitled to receive information have independent powers of collection (see Bock, in: Geppert/Piepenbrock/Schütz/Schuster, *Beck'scher Kommentar zum TKG*, 3rd. ed. 2006, § 112, marginal no. 28, § 113 marginal nos. 9 ff.; Graulich, in: Arndt/Fetzer/Scherer, *TKG*, 2008, § 112, marginal nos. 8, 18; Kleszczewski, in: Säcker, *Berliner Kommentar zum TKG*, 2nd ed. 2009, § 113, marginal no. 4).

125

## II.

The duty of storage of § 111 TKG is constitutionally unobjectionable to create a data basis for the information procedures laid down in § 112 and § 113 TKG.

126

1. § 111 TKG is not objectionable with regard to procedural constitutionality. Under Article 73.1 no. 7 of the Basic Law, the federal legislature is competent to pass the legislation.

127

However, the only direct authorisation given by Article 73.1 no. 7 GG is to organise the technical aspect of the installation of a telecommunications infrastructure and of the transmission of information with the aid of telecommunications equipment. The statute does not cover provisions directed to the transmitted content or the manner of use of telecommunications and, for example, telecommunications surveillance for the purpose of obtaining information for duties of criminal prosecution or of warding off dangers. With regard to legislative competence, each such provision is to be seen as relating to the area of law for whose purposes the surveillance is provided (see BVerfGE 113, 348 <368>; 125, 260 <314>). 128

In connection with the provisions of the Telecommunications Act, however, the federal legislature is not prevented, when the factual connection requires it, from legislating on requirements of data protection law at the same time, provided that this avoids a division between the technical and data protection provisions on data processing which creates incongruence. These provisions include not only provisions on the protective requirements, but as the obverse of these also provisions on what data may or must be kept available or supplied for the performance of government duties. In this connection, admittedly, the legislative competence of the federal legislature extends only as far as is required under the aspect of data protection law and the associated constitutional requirements. The Federation may therefore not base the authorisations for the actual data retrieval on Article 73.1 no. 7 of the Basic Law. It needs an independent legal basis for this, or else it must leave the decision on it to the *Länder* (see BVerfGE 125, 260 <315>). 129

Proceeding on this basis, there are no objections to § 111 TKG. This provision imposes on the telecommunications service providers a duty to collect and store particular telecommunications-related customer data in order to keep these available the performance of government duties. Understandably, such a provision may only be made in connection with the telecommunications law requirements for data processing and data protection, and therefore by the federal legislature under Article 73.1 no. 7 of the Basic Law. 130

2. Substantively too, § 111 TKG satisfies the constitutional requirements. The scope of the duty of storage – subject to the requirement of adequate legal bases for the retrieval and the further use of the data – is compatible with the requirements of the principle of proportionality. 131

a) § 111 TKG serves to maintain a reliable data basis for information which permits particular authorities to attribute telecommunications numbers to individual subscribers. The improvement of government performance of duties intended by this, in particular in the area of criminal prosecution, the warding off of dangers and intelligence activities, is a legitimate purpose, which may justify an encroachment upon the right to informational self-determination. 132

The fact that the data covered by § 111 TKG are to be kept available by way of precaution without occasion is not an illegitimate objection which cancels the right to in- 133

formational self-determination itself. Article 2.1 in conjunction with Article 1.1 of the Basic Law does not prohibit every precautionary collection and storage of data whatsoever, but merely lays down special requirements for the justification of such precautionary data collections and subjects them to a restrained formulation (see BVerfGE 125, 260 <317>). In contrast, the 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>; 125, 260 <317>). But the present case does not relate to such a storage of data, which is as a matter of principle impermissible. On the contrary, in § 111 TKG the legislature lays down a selective retention of particular data, restricted in their scope and with a precisely defined information content, for the purposes defined in detail in §§ 112, 113 TKG. The supply structured in this way of a data basis for specific information is not subject to this strict prohibition of data retention.

b) The collection and storage of the data governed by § 111 TKG is suitable to achieve the legislative objective. § 111 TKG creates a data basis in order to be able to attribute telecommunications numbers to their subscribers under §§ 112, 113. Admittedly, these data do not reveal who actually uses or has used the respective connection as a party to telecommunications. At all events, however, the relevant data are clearly suitable as the starting point for further investigations. It is not necessary that the goal of the legislation is actually attained in every case; for it to be suitable, it is merely necessary that the attainment of the goal is facilitated (see BVerfGE 63, 88 <115>; 67, 157 <175>; 96, 10 <23>; 103, 293 <307>; 125, 260 <317-318>). The provision therefore does not fail the test of suitability for the reason that criminal offenders who wish to circumvent the provision sometimes use telecommunications services anonymously, under false names or with mobile phone cards acquired from third parties, or because the customer data given by the users with regard to email services remain unexamined and may therefore be false. 134

c) The duty of storage of § 111 TKG is necessary to make reliable information possible. Admittedly, the data governed by § 111.1 TKG are predominantly stored by the service providers in any case to conduct their contractual relationships under § 95 TKG. But § 111.1 TKG also ensures that data are available in cases in which their storage is not necessary for the providers to conduct contractual relationships, as is the case in particular with customers who use prepaid mobile phone cards. 135

d) § 111 TKG does not violate the requirements of proportionality in the narrow sense. Even if the provision orders a precautionary collection and storage, without occasion, of a great range of telecommunications data, in view of the relatively restricted information content of the collected data this is an encroachment of limited weight. 136

aa) However, the encroachment is non-trivial. It has weight insofar as § 111 TKG makes it possible to attribute telecommunications numbers and subscribers almost completely for all telecommunications services and for this purpose individualising data such as address, date of birth and date when the contract commences are 137

recorded and kept available by the government. The data form a general basis for information and fulfil the function of a telecommunications number register. As a rule, they make it possible to obtain all the telecommunication numbers of any person; conversely, virtually every telecommunications event for which a telecommunications number is determined may also be attributed to a connection and thus to a subscriber. As data which relate to the fundamental elements of telecommunications events they are therefore associated with particularly protected information relationships whose confidentiality is essential for a free order. In addition, the corresponding data are collected and stored without cause by way of precaution in order to make them available for the performance of government duties.

bb) Nevertheless, the encroachment constituted by this is not of very great weight. In particular, the fact that the data are collected by way of precaution does not give the procedure a very great weight. For even if § 111 TKG has a great range, the encroachment is restricted in substance to narrowly restricted data which in themselves give no evidence as to the specific activities of individuals and whose use the legislature has restricted to purposes defined in more detail. In such cases, even a precautionary storage is not automatically a particularly serious encroachment for the mere reason that it is carried out without occasion. Admittedly, the precautionary storage of data must always remain an exception to the rule and needs to be justified (see BVerfGE 125, 260 <317>). But it is not excluded from the outset that precautionary data collections may be justified as the basis of the performance of a variety of government duties, such as are currently familiar in the form of the register of residents or, in the field of motor vehicles, in the form of the Central Vehicle Register (*Zentrales Fahrzeugregister*) and the Central Register of Driving Licences (*Zentrales Fahrerlaubnisregister*) (see § 2 Framework Act on Registration (*Melderechtsrahmengesetz – MRRG –*; § 33 and § 50 Road Traffic Act (*Straßenverkehrsgesetz – StVG –*)). The fact that here, the state obliges private persons to collect data on its behalf does not change this.

138

The data covered by § 111 TKG have limited probative value. They merely make it possible for telecommunications numbers to be individually attributed to the respective subscribers and thus to those numbers' potential (and typical) users. These data contain no more detailed private information. In a fundamentally different way than in the case of precautionary storage of all telecommunications traffic data (see BVerfGE 125, 260 <318 ff.>), neither do these data as such contain highly personal information, nor is it possible to use them to create personality profiles or track users' movements. Nor does § 111 TKG cover dynamic IP addresses. In the current technical conditions, in which static IP addresses are allocated only to a very limited degree and normally to large-scale institutional users, this does not enable an extensive attribution of internet contacts, even if static IP addresses were to be regarded in non-constitutional law as line identification numbers within the meaning of § 111.1 sentence 1 TKG. However, if the allocation of static IP addresses were to be used more extensively, for example on the basis of Internet Protocol Version 6, the provision

139

might acquire considerably more weight as an encroachment (see C. III. 2. c below).

Nor does a particular weight of the encroachment result from the fact that the data of § 111 TKG, taken in context, permit individual telecommunications events known to the authorities to be attributed and thus in certain circumstances make it possible to obtain individualised knowledge of their circumstances or their content. For in this way all that is made possible from the outset is the investigation of individual events where required by a specific case. In these cases, the authority already knows the circumstances or the content of the telecommunications event which is to be individualised with the data of § 111 TKG, whether because the authority has found them by investigation within its own competence – for example on the basis of § 100g of the Code of Criminal Procedure (*Strafprozessordnung* – StPO) – involving encroachment upon the secrecy of telecommunications, whether because it has learnt of them through its own observations or from third-party information without such an encroachment. In the same way, conversely no particular weight of the encroachment results from the fact that a retrieval of telecommunications numbers may be followed by further measures which in certain circumstances may entail serious encroachments, including encroachments upon the secrecy of telecommunications. For such further encroachments are only permissible under independent legal bases, which must take account of the weight of the encroachment in question.

140

cc) The possibility of attribution of the data collected in § 111 TKG serves the effective performance of the duties of the authorities defined in more detail in the provisions on use. It is constitutionally justified by the fact that the state may have a legitimate interest in successfully investigating particular telecommunications events if occasion arises, and this interest in the performance of particular tasks may have considerable weight, in individual cases even pre-eminent weight. It may not be cited in opposition to this that direct communication without means of telecommunications has no comparable encroachments. For the situation in that case is different. Because direct communication does not resort to technical means of communication which make it possible, without public observation, to interact over any distance in real time, it has no comparable basis, nor is there a comparable necessity for such a register. The traditional powers of investigation, for example the examination of witnesses or the seizure of documents, are more useful for clarification here than they are with regard to communication by means of electronic services. However, it is correct that even the possibilities of the modern means of telecommunications provide no justification for registering, if possible, all activities of citizens by way of precaution and making them basically reconstructible in this way (see BVerfGE 125, 260 <323-324>). But there is no question of this when a register of telecommunications numbers is established, even when account is taken of the interaction with other available data.

141

3. Since the extent of the data to be stored under § 111 TKG – irrespective of the constitutional requirement that their further use should not be disproportionate – is constitutionally unobjectionable and the Federal Republic of Germany can thus at the

142

same time satisfy the requirements of European Union law, further questions relating to the law of the European Union are not relevant for the decision on the constitutional complaint.

### III.

§ 112 TKG is also constitutionally unobjectionable. 143

§ 112 TKG governs the use of the data stored under § 111 TKG in the form of an automated information procedure in which the Federal Network Agency is to transmit the data on request to particular authorities named in § 112.2 TKG. The provision is the legal basis only for the duty to make the data available as customer databases, for access to and transmission of these data, but not also for the retrieval in the form of a request from the authorities entitled to receive information. But in this connection – in conformity with current practice – it may be understood to the effect that the general entitlement to collect data of the authorities entitled to receive information may be sufficient for a request under § 112.4 TKG. Neither the system of competencies of the Basic Law nor the principle of proportionality prevents this. 144

1. § 112 TKG does not violate the system of competencies of the Basic Law. The federal legislature was entitled to legislate for the automated information procedure, including the definitive order of a duty of the Federal Network Agency to transmit data, on the basis of its competence for telecommunications law under Article 73.1 no. 7 GG. 145

a) However, in this connection too the federal legislature may only rely on a legislative competence by virtue of a factual connection. Accordingly, the federal legislature is restricted to legislating for data protection provisions which can sensibly only be legislated on only in connection with the provisions for the creation of a telecommunications infrastructure and for informational self-determination (see BVerfGE 125, 260 <314>). These include, in addition to provisions to protect the data, conversely also provisions which define the limits of this protection and lay down the conditions under which and the purposes for which data are made available for the performance of government duties. 146

Article 73.1 no. 7 of the Basic Law thus does not authorise the federal legislature to legislate in full on data exchange between authorities, but it does permit it to pass provisions which, giving release from the requirements which serve to protect the data, at the same time conversely lay down the possible purposes of a use of data for the performance of government duties. The federal legislature can therefore determine the requirements subject to which an authority may transmit data (data transmission authorisation). But with regard to the transmission of data between authorities, which is a form of mutual administrative assistance, this includes the decision, which is final and determinative both for the authority subject to a duty and also indirectly for the persons whose data are affected, for what purposes and in what cases the data must be transmitted on request (data transmission duty). In the area of telecommunications 147

law, the responsibility in the law relating to competence for the data transmission of an authority, in particular a federal authority, is that of the Federal Government.

In contrast, the legislative competence ends where the retrieval of such information is concerned. The authorizations for data retrieval itself need an independent legal basis or must be left to the *Länder* (see BVerfGE 125, 260 <315>). 148

b) Proceeding on this basis, there are no objections to § 112 TKG under the law relating to competencies. 149

aa) As stated, § 112 TKG is not to be understood as legislation in full which at the same time supplies the legal basis for the requests of the specialised authorities and of the courts, which is a necessary requirement of the provision (see C. I. 2. b above)). Using the image of the double door, § 112 TKG opens the door of transmission, but not also the door of data collection by the specialised authorities. 150

bb) In contrast, § 112.4 TKG – in addition to making the data available in § 112.1 TKG and authorising access to these data – provides on the one hand for the authority to transmit data and in connection therewith defines their purpose and their potential target group. On the other hand, it also provides for a duty of transmission on the part of the Federal Network Agency. Since the provision creates an exchange of data between authorities, but not a duty of private persons to supply information, this is constitutionally unobjectionable. Accordingly, conversely, a sufficient legal basis for a request by the authorities desiring information is also provided by provisions which merely give general authority to collect personal data but in themselves do not create a duty of information. 151

(1) In § 112 TKG, the legislature provides for an exchange of information between authorities. In contrast to the demand under § 113.1 TKG, a request under § 112.4 sentence 1 TKG is defined not as a desire for information addressed to the individual telecommunications service provider, but as a desire for information addressed to the Federal Network Agency itself, which not merely transmits the information, but itself issues it. As a result, the Federal Network Agency, in a similar way to the Federal Motor Transport Authority (*Kraftfahrt-Bundesamt*) in the field of vehicle and vehicle owner data and of the data relevant to driving licences, is directed to keep the attribution of telecommunications numbers and other line identification numbers available for public purposes in the form of a register and to supply information on this. The fact that the data are not stored by the Federal Network Agency itself, but by the enterprises, which make them available for retrieval by the authority, does not alter this in any way. On the contrary, this is only a different technical form of administration of numbers by the Federal Network Agency. This is made clear by the fact that the data are made available in a form laid down in detail and standardised by the Federal Network Agency and their retrieval and transmission are then carried out by the latter direct to the requesting authorities, not only without any collaboration, but without the knowledge of the telecommunications enterprises. 152



(2) Since § 112.4 TKG in this way relates to the exchange of data between authorities, it is unobjectionable in the law on competence that it itself directly governs the duty of transmission of the data stored under § 111 TKG with regard to the Federal Network Agency. It corresponds to this that a mere authorisation of simple collection of data is sufficient as a legal basis for the retrieval of data by the authority requesting information; such an authorisation is contained, for example, in § 26 of the Rhineland-Palatinate Police and Regulatory Authorities Act (*Polizei- und Ordnungsbehörden-gesetz Rheinland-Pfalz* – PolG RP), Article 31 of the Bavarian Police Duties Act (*Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei* – PAG), § 13.1 of the Hesse Act on Public Security and Order (*Hessisches Gesetz über die öffentliche Sicherheit und Ordnung* – HSOG), or for the area of the protection of the constitution in Article 5 of the Bavarian Act on the Protection of the Constitution (*Bay-erisches Verfassungsschutzgesetz* – BayVSG) and § 4.1 of the Saxony Act on the Protection of the Constitution (*Sächsisches Verfassungsschutzgesetz* – SächsVSG). No more extensive enabling legislation is therefore needed to create specific information duties. 153

(3) Ultimately, therefore, § 112 TKG is similar to full legislation on such information, *inter alia* with regard to authorities whose activities are to be defined by *Land* legislation. For if even simple provisions on data collection are sufficient as a legal basis for the information requests under § 112 TKG – these are available to virtually all authorities which process personal data – this means that the legislation on information also takes effect in matters which are governed by *Land* law, without a separate decision of the *Land* legislature relating to telecommunications law. However, this is unobjectionable in the law on competence. For the right of the *Länder* to make the final decision on whether and how data are to be retrieved is unaffected in these cases. Since the requests for information have to have a legal basis which is separate from § 112 TKG and which may be *Land* law, the *Länder* are free themselves to draft and to flesh out these requests in the areas of legislation reserved to the *Länder* – in particular, for example, in police law – for the retrieval of the data under § 112 TKG. 154

2. § 112 TKG satisfies the requirements of the principle of proportionality. The provision serves to increase the effectiveness of the performance of their duties by the authorities named in § 112.2 TKG and it is suitable and necessary for this. It is also proportionate in the narrow sense. 155

a) However, the provision acquires a considerable weight of encroachment from the fact that § 112 TKG very much simplifies the data retrievals. The procedure, which is centrally organised and automated, permits an access which largely removes practical difficulties of data collection and makes the data of the persons affected available without delay or attrition in the form of requirements of review. In addition, the information is given without telecommunications enterprises or other third parties becoming aware of this. Admittedly, the fact that the issuing of information is not noticed by the telecommunications enterprise ensures discretion for the persons whose data are involved (see BVerfGE 118, 168 <199>); but at the same time, this means that the 156

encroachments lack the effects of restraint and control which are entailed by observation by third parties. In addition, a legal review by the Federal Network Agency, which transmits the data, is only made if there is a particular occasion for this (see § 112.4 sentence 2 TKG). Since the retrieving authority does not have to give reasons for its request, however, such an occasion will scarcely ever arise.

Weight also attaches to the fact that the legislature has drafted the purposes of the data very broadly. The data may generally be transmitted to the authorities named in § 112.2 TKG for the performance of their statutory duties. This is restricted only for the law enforcement authorities under § 112.2 no. 2 TKG and under § 112.2 nos. 3 and 7 TKG for the customs authorities named there. But it is important in this connection that data may be issued to the former, under § 112 TKG, only for purposes of warding off danger, which excludes mere risk precaution. In connection with the respective duties of the authorities entitled to retrieve, the information duties of the Federal Network Agency are also not very restricted. In particular, there are no strict encroachment thresholds in the statute; instead, the duty of information is opened in full to the respective competence of the authorities. However, the fact that information may only be given insofar as it is necessary for the performance of the duty does create an objectively limiting factor. This ensures that retrievals are not casually permitted for mere guidance in advance but only when information actually needed for the performance of duties cannot be obtained more easily but equally effectively in another way.

157

b) Despite the fact that the weight of the encroachment is considerable, the provision is proportionate. The authorities entitled to retrieve are at least limited in number. The purposes for which they are given information under § 112.2 TKG are central duties relating to the guarantee of security. In view of the increasing importance of electronic means of communication and the concomitant changes of human communication behaviour in all areas of life, the authorities here depend to a great extent on a possibility which is as uncomplicated as possible of being able to attribute telecommunications numbers individually. In this respect, it is a decision of the legislature which is constitutionally unobjectionable if it permits the transmission of these data in order to investigate criminal offences and dangers, to observe developments which endanger the constitution in order for the government and the public to be informed or to give assistance in emergencies. Because such investigations must often be carried out rapidly and without the knowledge of those affected, an automated information procedure is of particular importance for them. Increasing the effectiveness of the work of the courts is also a concern whose weight is supported by such a provision.

158

The limited probative value of the data is of central importance for the weighing of interests (see above C. II. 2. d) bb): They provide information solely on the attribution of individual telecommunications numbers to their subscriber. Even if, in specific collection contexts, sensitive information may result from them, the information content of this information as such remains limited and in addition depends on further investigations whose lawfulness is to be evaluated under different provisions.

159

c) Nor is the provision disproportionate in the present state of technological development and practice on the grounds that – depending on the interpretation of the concept of a line identification number in § 111.1 TKG – in certain circumstances it makes it possible to identify static IP addresses. For at present, no static IP addresses are allocated to private users as individual customers as a general rule, and consequently these private users are at all events not affected. On the contrary, individual customers are normally allocated IP addresses only for the current session, that is, as dynamic IP addresses. However, the concept of line identification number of § 111 TKG does not cover dynamic IP addresses, and therefore § 112 does not enable these to be de-anonymised. The allocation of static IP addresses, whose attribution is at present in any case publicly accessible in practice, is essentially restricted to institutions and large-scale users. The possibility of retrieving such numbers has little weight in these circumstances.

160

However, § 112 TKG may acquire substantially greater weight of encroachment if static IP addresses in future – for example on the basis of Internet Protocol Version 6 – should become more widely used as the basis of internet communication. For the question of the weight of encroachment of the identification of an IP address does not primarily depend – even if a number of fundamental rights apply in this case – on whether an IP address is technically dynamic or static, but on the actual significance of the creation of a duty of information in this connection. But if in practice static IP addresses are allocated to a great extent to private persons too, this may possibly mean that the identities of internet users are broadly or at least largely determined and that communications events in the internet are de-anonymised not only for a limited period of time, but permanently. Such a far-reaching possibility of de-anonymisation of communication in the internet goes beyond the effect of a traditional telephone number register. Admittedly, the information on the allocation of an IP address to a subscriber does have a certain similarity to the identification of a telephone number. Here too possible further information content – going beyond the mere allocation of the IP address – cannot be derived from the information itself, but only transpire in connection with knowledge which the authority has already obtained elsewhere or may in future obtain through its own legal activities. Nevertheless, the weight for the person affected of the attribution of an IP address to a subscriber may not be equated to that of the identification of a telephone number, because the former makes it possible to access information whose scope and content are substantially more far-reaching (see BVerfGE 125, 260 <342>). In view of this increased information potential, the general possibility of the identification of IP addresses would only be constitutionally permissible subject to narrower limits (see BVerfGE 125, 260 <343-344, 356 ff.>). The legislature has a duty to observe and where appropriate to make corrections in this connection.

161

d) § 112 TKG is also not disproportionate or indefinite merely because it imposes no further requirements for the retrieval provisions of non-constitutional law to be more specific.

162

However, § 112 TKG does not in fact restrict information to retrievals which are legit-  
imised by specific legal bases relating to the automated information procedure, but al-  
so accepts requests which are based on simple powers of data collection. As a result,  
there is no requirement on the non-constitutional level for the entitled authorities to be  
expressly specified over and above § 112.2 TKG and for further conditions for data  
retrieval which are to be observed. But this is constitutionally unobjectionable. Since  
the subject here is the transmission of data by an authority and the substantive condi-  
tions for this, including those with regard to the persons whose data are involved, are  
laid down definitively and with sufficient clarity by § 112 TKG, then, taking account of  
the limited weight of encroachment of the provision, this is compatible with the princi-  
ple of proportionality and corresponds to the structure of the provisions on the auto-  
mated retrieval of vehicle and vehicle owner data from the vehicle register (§§ 35 ff.  
StVG) and the provision on data transmission in the law relating to the registration of  
residents (§ 18 MRRG). Admittedly, this does not change the responsibility of the leg-  
islature – and in this connection, where applicable, of the *Länder* – for the constitu-  
tional formulation of the data collection provisions, which are not themselves the sub-  
ject of the present proceedings. In addition, this does not relieve the public authorities  
responsible from the duty to apply these provisions in such a way that specific ac-  
count is taken of the requirements of § 112.1 and 112.2 TKG and in particular of the  
requirement that collection must be necessary even in the individual case, and of the  
further requirements of the principle of proportionality.

163

#### IV.

§ 113.1 sentence 1 TKG is constitutionally unobjectionable. However, the provision  
must be interpreted in conformity with the Basic Law. Both for reasons of the law re-  
lating to competence and also for constitutional reasons, § 113.1 sentence 1 TKG  
must be interpreted in such a way that it in itself alone does not create duties of infor-  
mation of the telecommunications enterprises. Instead, it requires separate non-  
constitutional enabling provisions – where applicable, in *Land* law – for the definitive  
justification of a duty of information; this legislation must in itself contain clear defini-  
tions creating a duty of the telecommunications service providers towards the authori-  
ties entitled to retrieve in each case. In addition, § 113.1 sentence 1 TKG may not be  
interpreted to the effect that it permits an attribution of dynamic IP addresses.

164

1. § 113.1 TKG is covered by the legislative conference of the federal legislature un-  
der Article 73.1 no. 7 of the Basic Law, provided it is interpreted in conformity with the  
Basic Law.

165

The competence of the federal legislature for data protection provisions follows from  
Article 73.1 no. 7 of the Basic Law by virtue of a factual connection; this competence  
also includes, as stated, the creation of provisions which provide for the potential use  
for the performance of government duties of the data stored by the telecommunica-  
tions enterprises. Under this competence, the federal legislature may authorise and –  
corresponding to a duty of information contained in non-constitutional law – also

166

oblige the telecommunications service providers to transmit such data to particular authorities, where there is an effective retrieval of data and for specific purposes which the federal legislature must lay down in detail (see BVerfGE 125, 260 <344 ff.>). In contrast, the authorisation for such a retrieval of data may not itself be based on the competence for telecommunications law, but must have a basis of competence in non-constitutional law.

Accordingly, a demand for information under § 113.1 TKG – as in § 112 TKG – also requires a separate legal basis in non-constitutional law. But unlike in the case of § 112 TKG, in which the federal legislature imposes on a federal authority the duty to supply information, the federal legislature cannot definitively create a duty, on the basis of Article 73.1 no. 7 of the Basic Law, for private telecommunications enterprises to comply with a desire for information. Instead, imposing a duty on private persons which at the same time obliges them to reveal their customers' data is not part of the definition of the limits of data protection, but an inseparable component of data retrieval. On the basis of Article 73.1 no. 7 of the Basic Law, the federal legislature may only provide for the opening up of the customer data for the performance of government duties, but not for the access to these data itself, and consequently the imposition of an obligation on the telecommunications service providers as private persons holding information must be laid down in the retrieval provision in subject matter which is reserved to *Land* legislation. A legal basis which merely permits data relating to freely accessible information to be collected, but does not itself create an information duty of third parties, is insufficient for this purpose (examples are § 26 of the Rhineland-Palatinate Police and Regulatory Authorities Act; Article 31 of the Bavarian Police Duties Act; § 13.1 of the Hesse Act on Public Security and Order; Article 5 of the Bavarian Act on the Protection of the Constitution; § 4. 1 of the Saxony Act on the Protection of the Constitution). Accordingly, in the light of the system of competencies of the Basic Law, § 113.1 TKG must be interpreted to the effect that for demands for information in areas where legislation is reserved to *Land* law it requires specific legal bases in *Land* legislation which independently create a duty of information of the telecommunications enterprises.

167

2. The principle that provisions must be clearly drafted has a specific function in connection with encroachments upon the right to informational self-determination; in this respect too, § 113.1 TKG is to be interpreted to require specific legal bases for data retrieval in the form of a demand for information addressed directly to private third persons, where these legal bases must independently create an information duty of the telecommunications enterprises. Consequently, strict retrieval provisions are also required for federal subject matter which goes beyond a mere authority to collect data.

168

a) If a statutory provision gives authority for an encroachment upon the right to informational self-determination, the requirement of definiteness and clarity also has the specific function of ensuring that the purpose of use of the information in question must be defined with sufficient precision. This reinforces the constitutional require-

169

ment that the use of the information collected must be limited to specific purposes (see BVerfGE 118, 168 <187>; 120, 378 <408>). The occasion, purpose and extent of the given 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, 372>; 113, 348 <375>; 125, 260 <328>; established case-law). In the case of forms of information exchange which are graduated or consist of several encroachments, the requirement of clearly drafted provisions applies to each stage.

b) § 113.1 sentence 1 TKG satisfies these requirements if it is merely understood as a release provision which lays down in what cases the telecommunications enterprises are entitled to transmit the data in question - and also obliged, where a demand is made which is independently laid down in non-constitutional law and is effective. Admittedly, the provision defines the potential purposes of such a transmission very broadly, but with sufficient precision. As a provision which initially only lays down the potential purposes of the data, it satisfies the constitutional requirements of definiteness if the duties whose performance the supply of information is to legitimise are only described in abstract terms and independently of specifically entitled authorities.

170

c) In contrast, § 113.1 sentence 1 TKG cannot be so understood that it itself creates all the requirements for data retrieval with the result that all authorities solely on the basis of their simple entitlement to collect data are entitled to information under § 113.1 TKG. Admittedly, the legislature is in principle at liberty to deal with the entitlements of transmission and retrieval in the same provision. However, the federal legislature did not make such a provision in § 113.1 sentence 1 TKG. It does not even have the competence to legislate on subject matter in relation to which legislation in non-constitutional law is reserved to the *Länder* (see above C. IV. 1.). But even for subject-matter in relation to which the federal legislature has the competence to legislate in non-constitutional law, § 113.1 sentence 1 TKG does not provide with sufficient precision that the provision is to be understood as a retrieval provision in this connection. Instead, the federal legislature based the provision of § 113 TKG solely on its competence for telecommunications law (BTDrucks 15/2316, p. 55), which does not support the creation of such a retrieval provision, as set out above. In addition, the group of authorities entitled to retrieve, and thus the range of the information duties, is restricted only in relation to the authorities' duties, and thus not restricted with sufficient precision. Instead, the creation of information duties of private persons requires clear provisions as to the authorities to which the providers are specifically to be obliged to transmit data. Only this also justifies to the persons whose data are involved the encroachment upon the right to informational self-determination. But such a provision is made by neither § 113.1 sentence 1 TKG itself nor the provisions – such as § 8. 1 of the Federal Act on the Protection of the Constitution (see Droste, *Handbuch des Verfassungsschutzrechts*, 2007, pp. 230-231) or § 21.1 of the Federal Police Act (*Bundespolizeigesetz* – BPolG) – which merely contain an entitlement to collect data without an express information duty towards third parties make such a

171

provision.

3. § 113.1 sentence 1 TKG must in addition be interpreted in conformity with the Basic Law to the effect that it cannot be seen to contain a legal basis for the attribution of dynamic IP addresses. 172

Recourse to § 113.1 sentence 1 TKG to identify dynamic IP addresses is out of the question for the mere reason that this is to be defined as an encroachment on Article 10.1 of the Basic Law (see above C. I. 1. a) cc). Such encroachments are subject to the citation requirement of Article 19.1 sentence 2 GG, which requires the legislature to name the fundamental right upon which an encroachment is made and to state the number of the Article in which it is contained. This is lacking in the present case. 173

Apart from this, however, an identification of dynamic IP addresses on the basis of § 113.1 sentence 1 TKG is also out of the question because the provision does not define such an authorisation with sufficiently clear provisions. The identification of dynamic IP addresses makes it possible to a broad extent for communication events in the internet to be de-anonymised. It is true that this has a certain similarity to the identification of a telephone number. However, in its very scope, but above all in the content of the contacts on which it can supply information, it has a substantially greater personal relevance and cannot be regarded as equivalent to identifying a telephone number (see BVerfGE 125, 260 <341 ff.>). In this connection, a sufficiently clear decision of the legislature is necessary as to whether and subject to what requirements such an identification is to be permitted. However, such a decision cannot be inferred with sufficient clarity from § 113.1 sentence 1 TKG. The provision does not expressly deal with this question. Nor can a sufficiently clear statement be inferred from § 113.1 sentence 1 TKG by interpretation. § 113.1 sentence 1 TKG names only § 95 and § 111 TKG as the subject of the information duty, but it does not show that the telecommunications enterprises, when they prepare such information, might also be entitled and obliged to evaluate the traffic data under § 96 TKG; at all events, the final formulation of the purposes of the traffic data in § 96 TKG does not support this interpretation. Accordingly, the question has also long been controversial in case-law and literature too (see above A. I. 3.). § 113.1 TKG therefore does not contain a sufficiently clearly defined authorisation to identify dynamic IP addresses in addition. 174

4. On the basis of the above stipulations, § 113.1 sentence 1 TKG is compatible with the Basic Law. In particular, it satisfies the requirements of the principle of proportionality. § 113.1 TKG is the basis for an information procedure which makes it possible to attribute telecommunications numbers to assist the security authorities' performance of their duties. For this, the provision is not merely suitable and necessary, but also structured with restraint in a constitutionally acceptable manner. 175

a) However, § 113.1 sentence 1 TKG opens the manual information procedure very wide. It permits information for the purpose of warding off dangers, prosecuting criminal offences or regulatory offences and performing intelligence duties. In this connection, the provision is also given no specific thresholds of encroachment which define 176

its scope in more detail. Instead, it always permits information in the individual case if this is necessary to perform the above duties.

However, in view of the information content of the data in question, which in itself is limited, and their great importance for an effective performance of duties, the reach of this provision is constitutionally unobjectionable. In this connection, account must be taken of the fact that it by no means permits information to be given indiscriminately. On the contrary, there is a restrictive effect in the fact that information under § 113.1 sentence 1 TKG are called for in the individual case and must be necessary. In relation to warding off danger, which the legislature has expressly not defined as including risk precaution, a prudent interpretation reveals that a “concrete danger” within the meaning of the “general clauses” (*Generalklauseln*) of police law is a requirement for such information. Admittedly, this threshold is low and also admits the suspicion of dangers. Equally, it does not in advance restrict information to persons endangering public security within the meaning of general police and regulatory law. However, this does not relieve it from restriction to such an extent as to be disproportionate in view of its limited weight of encroachment. In particular it does not enable information as a general means for lawful administrative enforcement, but in the individual case it requires the duty in question to have a security-law character. It is true that in regard to the intelligence services, which in general act in advance, irrespective of concrete dangers, there is no comparable threshold of encroachment. But this is justified by the restricted duties of the intelligence services, which are not directly aimed at police measures, but only at a duty to provide reports to the politically responsible state bodies or to the public. Apart from this, it follows here too from the requirement of necessity in the individual case that information under § 113.1 sentence 1 TKG must be required in order to successfully investigate a particular action or group which requires observation by the security authorities. Insofar as information relates to the prosecution of criminal offences and regulatory offences, the requirement of necessity in the individual case means that there must at least be an initial suspicion.

177

Taken together, these thresholds are not high, but they are constitutionally acceptable. In this connection, it must be taken into account in comparison to § 112 TKG that a manual information procedure entails certain procedural efforts on the part of the retrieving authority, which is likely to encourage the authority to obtain the information only where it is sufficiently needed.

178

b) § 113.1 sentence 1 TKG is not disproportionate by reason of the fact that in addition to the data covered by § 111.1 TKG it also includes the data under § 95 TKG in the duty of information. The legislature is in principle not prevented from permitting access to further telecommunications data – not covered by § 111 TKG – which the telecommunications enterprises store to perform their contracts. § 111 TKG is intended to secure a minimum amount of data. But this does not exclude the possibility that in a dynamic sector like telecommunications other data may also be important for the performance of government duties and may be made accessible. It need not be decided here whether or how far the duties of information also extend to information

179



which is not related to telecommunications. For the complainants do not submit in a substantiated manner in what way they would be affected by this.

c) Finally, the broadness of the circle of persons with a duty of information also encounters no objections. The statutory provision is clearly designed to be able to attribute if possible all telecommunications numbers to their respective subscribers (and in addition, ultimately, if possible, to their users). This is justified in view of the aim of making investigations more effective. The fact that in this connection commercial providers, for example of Wi-Fi hotspots or in hotels, are in principle included does not violate the principle of proportionality. In addition, the requirements contained in § 113.1 sentence 1 TKG and the procedural efforts which such an information procedure entails also ensure that the data are only accessed in the case of information of a certain importance. 180

## V.

The constitutional complaint is well-founded insofar as it challenges § 113.1 sentence 2 TKG. 181

1. However, § 113.1 sentence 2 TKG is not subject to constitutional objections for the mere reason that it permits access to the access protection data subject to the provision. Here too there is an encroachment upon the fundamental right to informational self-determination which is capable of justification under general principles. In this connection, the same applies with regard to the requirements of the relationship to non-constitutional law which follow from the system of competencies and the principle of the rule of law as applies to § 113.1 sentence 1 TKG (see above C. IV. 1. to 3.). 182

2. However, § 113.1 sentence 2 TKG does not satisfy the requirements which follow from the principle of proportionality. It is true that the state has a legitimate interest in making the data named in § 113.1 sentence 2 TKG accessible to the relevant authorities for their performance of their duties. But access to these data is not necessary in the degree provided by § 113.1 sentence 2 TKG for these authorities to perform their duties effectively. 183

§ 113.1 sentence 2 TKG relates to data which, as access codes (such as passwords, PINs or PUKs), protect the access to end user devices and storage installations and thus protect the persons involved against access to the relevant data or telecommunications events. The provision makes these data accessible to the authorities and thus puts the authorities in the position to surmount the relevant barriers. In doing so, however, it defines the supply of information on these codes independently of the requirements for their use. Instead, the question as to when the authorities may use the access codes and have access to the data and telecommunications events protected by them is determined under independent legal bases, as is expressly stated by § 113.1 sentence 3 TKG for encroachments upon the secrecy of telecommunications. The requirements for this differ here depending on the nature of 184

the encroachment both in procedural and substantive respects. If the use of the access code, for example, is to enable an online search or the monitoring of an ongoing telecommunications event, then depending on more details of the non-constitutional law involved, this requires the satisfaction of stricter substantive requirements and a judicial order or confirmation (see §§ 100a, 100b StPO; BVerfGE 120, 274 <332>). If, in contrast, a mobile phone has been seized and the code is then to be used to read the data stored on it, more generous encroachment thresholds may suffice for this (see BVerfGE 115, 166 <193 ff.>). Thus, for example, under the law of criminal procedure there is no need for a prior judicial order in the case of seizure and imminent danger (see § 98.1 StPO) and only subject to certain further requirements is a subsequent court confirmation needed (see § 98.2 StPO).

No reason is apparent for the authorities to be able to retrieve the access codes governed by § 113.1 sentence 2 TKG independently of the requirements for their use and thus in some circumstances subject to less stringent conditions. The collection of the access data governed by § 113.1 sentence 2 TKG, in view of the purposes pursued there, is necessary only if the requirements for their use are also satisfied. This is not sufficiently guaranteed by the provision of § 113.1 sentence 2 TKG in its present wording, since the retrieval of the access codes – for example in relation to criminal investigation proceedings – is always to be permissible subject to the requirements of § 161.1 StPO, even if the use of the data intended in the retrieval should be subject to further requirements, for example a prior judicial order. Conversely, however, the principle of proportionality does not require that the collection of the access codes should without exception be subject to the conditions which need to be satisfied for their most intensive (“maximum”) encroaching use. All that is necessary for effective criminal prosecution and warding off of danger is to subject the supply of information on such access protections to the requirements which are to be satisfied with regard to the purpose which they specifically intend in the retrieval situation.

185

## VI.

There are no further objections to the proportionality of the challenged provisions on the basis of the complaint. There has been no challenge that data security is not adequately guaranteed, nor can one be inferred from the submissions. Nor are there objections to the fact that in view of the slightness of the encroachment no specific proceedings of legal redress are intended against information under §§ 112 and 113 TKG. Legal redress in this connection may be sought under general rules – in particular together with legal redress proceedings against the final decisions of the authorities.

186

The requirements of the principle of proportionality do not give rise to a blanket requirement for the persons affected by the information to be notified of the information under § 112 and § 113 TKG, even on the level of the non-constitutional retrieval provisions, where such provisions should be located under the law of competencies (see BVerfGE 125, 260 <346-347>). It is not the subject of the present proceedings to de-

187

termine whether duties of notification or further measures such as the priority of data collection from the person affected in particular cases might better be contained in the retrieval provisions themselves.

#### D.

##### I.

The unconstitutionality of § 113.1 sentence 2 TKG does not result in a declaration of nullity, but merely in the determination that it is incompatible with the Basic Law, together with the order that for a transitional period, but at the latest until 30 June 2013, it may continue to be applied if the requirements for the use of the data it covers are satisfied in the individual case. 188

A mere declaration of incompatibility, attended by a transitional continuation in effect of the unconstitutional provision, may be made if the immediate invalidity of the challenged provision would deprive the protection of paramount concerns of the public interest of its foundation and if weighing against the fundamental rights affected shows that the encroachment may be tolerated for a transitional period (see BVerfGE 33, 1 <13>; 33, 303 <347-348>; 109, 190 <235-236>). This is the case here. If 113.1 sentence 2 TKG were declared null and void, the result would be that even in the cases in which the authorities are lawfully entitled to have access to telecommunications data to prevent or punish serious violations of legal interests it would not be sufficiently ensured that they were in the position to do this. Since the unconstitutionality of § 113.1 sentence 2 TKG relates to an encroachment of limited weight and the Basic Law is not altogether opposed to supplies of information such as are created by this provision, this result is not acceptable even for a transitional period. Instead, it is sufficient to order that the provision is to continue in effect for a transitional period and to subject it to the proviso that the data named in the provision may only be collected if the requirements for their use are satisfied. 189

For the same reasons, a transitional provision is also needed with regard to the constitutional requirements of the interpretation of § 113.1 sentence 1 TKG, which, in contrast to the present practice – to which the legislature oriented itself in its various amendments of the Telecommunications Act and the Code of Criminal Procedure (see BTDrucks 14/7008, p. 7; 16/5846, pp. 26-27; 16/6979, p.46) – result in substantial restrictions in dealing with the provision. If these requirements came into effect immediately, there would be a large number of cases in which information on telecommunications numbers could no longer be given in a large number of cases until new, clearly drafted retrieval rules were issued in non-constitutional law. In addition, dynamic IP addresses could no longer be identified before a reform of the law. In view of the importance of such information for the successful investigation of dangers and criminal offences, the disadvantages of such a result are out of proportion to the provisional acceptance of a practice which, although it does not procedurally satisfy constitutional requirements, is in essence capable of justification. It is therefore neces- 190

sary, for a transitional period, but at the latest until 30 June 2013, to accept the application of § 113.1 sentence 1 TKG, even without specific retrieval provisions, on the basis of simple data collection powers. In addition, the provision may until that time be used as the legal basis for the identification of IP addresses.

II.

With regard to the question as to whether an attribution of dynamic IP addresses should be transitionally permissible on the basis of § 113.1 TKG, the decision was passed by six votes to two. 191

The decision on the reimbursement of expenses is based on § 34a.2 of the Federal Constitutional Court Act. 192

Kirchhof	Gaier	Eichberger
Schluckebier	Masing	Paulus
Baer		Britz

**Bundesverfassungsgericht, Beschluss des Ersten Senats vom 24. Januar 2012 -  
1 BvR 1299/05**

**Zitiervorschlag** BVerfG, Beschluss des Ersten Senats vom 24. Januar 2012 -  
1 BvR 1299/05 - Rn. (1 - 192), [http://www.bverfg.de/e/  
rs20120124\\_1bvr129905en.html](http://www.bverfg.de/e/rs20120124_1bvr129905en.html)

**ECLI** ECLI:DE:BVerfG:2012:rs20120124.1bvr129905