Headnotes

to the judgment of the First Senate of 27 February 2008

– 1 BvR 370/07 –

– 1 BvR 595/07 –

1. **The general right of personality (Article 2.1 in conjunction with Article 1.1 of the Basic Law (*Grundgesetz – GG*)) encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems.**

2. **The secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read is constitutionally only permissible if factual indications exist of a concrete danger to a predominantly important legal interest. Predominantly important are the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence. The measure can already be justified even if it cannot yet be ascertained with sufficient probability that the danger will arise in the near future insofar as certain facts indicate a danger posed to the predominantly important legal interest by specific individuals in the individual case.**

3. **The secret infiltration of an information technology system is in principle to be placed under the reservation of a judicial order. The statute granting powers to perform such an encroachment must contain precautions in order to protect the core area of private life.**

4. **Insofar as empowerment is restricted to a state measure by means of which the contents and circumstances of ongoing telecommunication are collected in the computer network, or the data related thereto is evaluated, the encroachment is to be measured against Article 10.1 of the Basic Law alone.**

5. **If the state obtains knowledge of the contents of Internet communication by the channel technically provided therefor, this shall only constitute an encroachment on Article 10.1 of the Basic Law if the state agency is not authorised to obtain such knowledge by those involved in the communication.**

6. **If the state obtains knowledge of communication contents which are publicly accessible on the Internet, or if it participates in publicly accessible communication processes, in principle it does not encroach on fundamental rights.**

FEDERAL CONSTITUTIONAL COURT

– 1 BvR 370/07 –

– 1 BvR 595/07 –

Pronounced

on

27 February 2008

Mr Kehrwecker

as Registrar of the Court Registry

IN THE NAME OF THE PEOPLE

In the proceedings
concerning
the constitutional complaint

1. a) of Ms W (…),

b) of Mr B (…),

- authorised representative: Rechtsanwalt Dr. Fredrik Roggan,
Müllerstraße 153, 13353 Berlin -

against § 5.2 no. 11 in conjunction with § 7.1, § 5.3, § 5a.1 and § 13 of the North Rhine-Westphalia Constitution Protection Act (*VSG NRW*) in the version of the Act Amending the Act on the Protection of the Constitution in North Rhine-Westphalia (*Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen*) of 20 December 2006 (Law and Ordinance Gazette of North Rhine-Westphalia (*GVBl NW*) 2006, p. 620)

– 1 BvR 370/07 –,

2. a) of Mr B (…),

b) of Dr R (…),

c) of Mr S (…)

- authorised representatives:

1. Rechtsanwälte Baum, Reiter & Collegen,
Benrather Schlossallee 121, 40597 Düsseldorf,

2. Rechtsanwalt Peter Schantz, Schaperstraße 10, 10719 Berlin,
authorised representative of the complainants re 2a and 2b -

against § 5.2 no. 11, § 5.3, § 7.2 and § 8.4 sentence 2 in conjunction with §§ 10, 11 and § 17.1 of the North Rhine-Westphalia Constitution Protection Act in the version of the Act Amending the Act on the Protection of the Constitution in North Rhine-Westphalia of 20 December 2006 (Law and Ordinance Gazette of North Rhine-Westphalia 2006, p. 620)

– 1 BvR 595/07 –

The Federal Constitutional Court – First Senate – sitting with the Justices

President Papier,

Hohmann-Dennhardt,

Hofmann-Riem,

Bryde,

Gaier,

Eichberger,

Schluckebier,

Kirchhof,

held on the basis of the oral hearing of 10 October 2007:

Judgment

1. **§ 5.2 no. 11 of the Act on the Protection of the Constitution in North Rhine-Westphalia (*Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*) in the version of the Act of 20 December 2006 (Law and Ordinance Gazette of North Rhine-Westphalia, page 620) is incompatible with Article 2.1 in conjunction with Article 1.1, Article 10.1 and Article 19.1 sentence 2 of the Basic Law, and is null and void.**
2. **This disposes of the complaints asserted by the complainants against § 5.3 and § 17 of the Act on the Protection of the Constitution in North Rhine-Westphalia.**
3. **The constitutional complaint of the complainant re 1b is rejected as unfounded insofar as it addresses § 5a.1 of the Act on the Protection of the Constitution in North Rhine-Westphalia.**
4. **In other respects, the constitutional complaints are dismissed as inadmissible.**

5. The *Land* North Rhine-Westphalia is ordered to reimburse the complainants three quarters of their necessary expenses.

Reasons:

A.

The subject-matter of the constitutional complaints are the provisions of the North Rhine-Westphalia Constitution Protection Act regulating, firstly, the powers of the constitution protection authority regarding various instances of data collection, in particular from information technology systems, and secondly, the handling of the data collected. 1

I.

The impugned provisions were largely inserted or amended by the Act Amending the Act on the Protection of the Constitution in North Rhine-Westphalia of 20 December 2006 (Law and Ordinance Gazette of North Rhine-Westphalia, p. 620). 2

1. Both constitutional complaints complain of the unconstitutionality of § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act. This provision empowers the constitution protection authority to carry out two types of investigative measures: Firstly, secret monitoring and other reconnaissance of the Internet (alternative 1), and secondly secret access to information technology systems (alternative 2). 3

a) The Internet is an electronic combination of computer networks. It hence consists of information technology systems, and can itself also be regarded as an information technology system. The difference between the two types of measure regulated in § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act relates to the external appearance of technical access to the information technology system. Secret reconnaissance of the Internet is understood to be a measure by which the constitution protection authority obtains knowledge of contents of Internet communication using the channel technically provided therefor. The Government of the *Land* North Rhine-Westphalia speaks of server-orientated Internet reconnaissance when referring to such measures. 4

Secret access to an information technology system is understood by contrast to be technical infiltration which for instance takes advantage of the security loopholes of the target system, or which is effected by installing a spy program. The infiltration of the target system makes it possible to monitor its use or to view the storage media, or indeed to control the target system remotely. The Government of the *Land* North Rhine-Westphalia refers to such measures as client-orientated reconnaissance of the Internet. However, the impugned provision does not contain an indication that it is exclusively orientated towards the server-client model in order to facilitate measures in the framework of a network structure. 5

b) Insofar as § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act grants powers to perform secret reconnaissance of the Internet, the provision initially regulates how knowledge is obtained of generally accessible communication contents by the constitution protection authority. One example of this would be the accessing of an open Web site on the World Wide Web using a Web browser. According to the reasoning of the Act, it is also intended to enable the constitution protection authority to participate in chats, auctions or exchange fora, or to discover concealed Web sites using a cover (see *Landtag* document (*Landtagsdrucksache – LTDrucks*) 14/2211, p. 17). It would also be conceivable, for instance, for the constitution protection authority to use a password obtained elsewhere – for instance from an informant or by means of so-called keylogging – in order to access an e-mail inbox or an access-protected Web site. In such a case, the constitution protection authority would also obtain knowledge of the contents of Internet communication externally via the channel provided therefor. 6

c) Secret access to information technology systems using technical infiltration, as regulated in § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act, is currently the subject of intensive discussion in the political arena and among legal circles under the heading of “online search/online surveillance” (see on the legal debate for instance Buermeyer, *Höchstrichterliche Rechtsprechung im Strafrecht – HRRS* 2007, p. 392; Hofmann, *Neue Zeitschrift für Strafrecht – NStZ* 2005, p. 121; Hornung, *Datenschutz und Datensicherheit – DuD* 2007, p. 575; Rux, *Juristenzeitung – JZ* 2007, p. 285; Schaar/Landwehr, *Kommunikation & Recht – K&R* 2007, p. 202; Schlegel, *Goltdammer’s Archiv für Strafrecht – GA* 2007, p. 648; Warntjen, *Jura* 2007, p. 581). Such measures were already executed in isolated cases by federal authorities without a specific statutory empowerment. Little is known of the nature of the practical execution of previous “online searches” or of their successes. The Presidents of the Federal Criminal Police Office (*Bundeskriminalamt*) and of the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*), who were heard by the Senate during the oral hearing, have not provided any information on this for lack of permission to provide appropriate testimony. The execution of such measures was moreover temporarily ceased when the 7

Federal Court of Justice (*Bundesgerichtshof*) ruled that the Code of Criminal Procedure (*Strafprozessordnung – StPO*) did not currently contain a legal basis for such measures (see Decisions of the Federal Court of Justice in Criminal Cases (*Entscheidungen des Bundesgerichtshofes in Strafsachen* – BGHSt) 51, 211).

aa) The *Land* provision to be reviewed here contains the first and so far the only explicit empowerment of a German authority to engage in “online searches”. It is currently the subject of dispute at federal level as to which authorities are to be empowered to carry out “online searches” and under what preconditions. In particular, it is being discussed at present to create such an empowerment for the Federal Criminal Police Office in the course of its task to avert dangers of international terrorism – which has been newly inserted into the Basic Law in the context of the so-called fed- 8

eralism reform (Article 73 no. 9a of the Basic Law).

bb) “Online searches” are to accommodate the difficulties in investigations emerging if criminal offenders, in particular those from extremist and terrorist groups, use information technology, and the Internet in particular, for communication and to plan and commit criminal offences. The Presidents of the Federal Criminal Police Office and of the Federal Office for the Protection of the Constitution stated during the oral hearing that information technology systems are also used in order to establish and maintain contacts worldwide to prepare violent terrorist acts. In particular if persons who are to be attributed to extremist or terrorist groups encrypt or conceal stored files and communication contents, investigations carried out using the classical methods such as seizing information technology systems and storage media, or network-based telecommunication surveillance, could be made considerably more difficult or indeed quite impossible. 9

Secret access to an information technology system can be very difficult (see below for instance Buermeyer, *Höchstrichterliche Rechtsprechung im Strafrecht* 2007, p. 154; Hansen/Pfitzmann, *Deutsche Richterzeitung – DRiZ* 2007, p. 225; Pohl, *Datenschutz und Datensicherheit* 2007, p. 684). This is the case in particular if the user of the target system has taken technical security precautions and regularly updates his or her operating system. In the view of the experts heard in the oral hearing, the person concerned can at present at any rate effectively prevent infiltration by some of the access modes under consideration. Such infiltration may at least be highly laborious, depending on the circumstances of the individual case. 10

If infiltration is successful, it offers several advantages to the investigation authority in comparison to traditional investigation methods. Because of the secrecy of access, the person concerned is not forewarned for the future, unlike for instance in the case of a house search, which is carried out openly. If the user of a computer only stores data in encrypted form, an “online search” may allow such data to be collected in unencrypted form. By infiltrating the computer, the authority may access the data as the user uses it at the time in question. The advantage of circumventing encryption technology is also significant to the surveillance of ongoing Internet communication. Insofar as such communication is encrypted as it takes place – this is in particular frequently the case with speech telephony – it can only be effectively monitored at the terminal. Longer-term surveillance of the use of the computer can largely circumvent the use of cryptographic technologies and other security precautions. What is more, volatile data such as passwords and further information on the usage pattern of the person concerned can be collected. This kind of information would hardly ever be possible to obtain using classical investigation methods. 11

d) § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act empowers the constitution protection authority to undertake the regulated measures in principle under the general preconditions for data collection of intelligence services arising from § 5.2 in conjunction with § 7.1 and § 3.1 of the North Rhine-Westphalia Constitu- 12

tion Protection Act. According to these provisions, it is required in principle that by these means information can be obtained on efforts or activities that are relevant to the protection of the constitution or the sources necessary to obtain such information. Insofar as measures according to the impugned provision constitute an encroachment on the secrecy of correspondence, post and telecommunication, or are equivalent to such encroachment in terms of their nature and grievousness, according to § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act, they are however only permissible under the preconditions of the Act Restricting the Secrecy of Correspondence, Post and Telecommunication, Article 10 Act (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* (*Artikel 10-Gesetz – G 10*)); below: Act re Article 10 of the Basic Law).

e) Only the complainants re 2 also address § 17 of the North Rhine-Westphalia Constitution Protection Act, which regulates the transmission of personal data by the constitution protection authority, in connection with measures according to § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act. 13

2. Both constitutional complaints further address § 5.3 of the North Rhine-Westphalia Constitution Protection Act. The subject-matter of this provision is the notification of the person concerned subsequent to the deployment by intelligence services of the means regulated in § 5.2 of the North Rhine-Westphalia Constitution Protection Act. Sentence 1 of this section contains an obligation to, in principle, notify, with regard to which sentence 2 makes provision for several exceptions. 14

3. Only the complainants re 1 address § 5a.1 of the North Rhine-Westphalia Constitution Protection Act. This provision empowers the constitution protection authority to obtain information from financial institutions on participants in payment transactions and on monetary movements and investments. The precondition is the existence of factual indications of grievous dangers to the interests protected by the constitution protection authority. 15

An empowerment to collect account contents was already contained in the Constitution Protection Act prior to the Amending Act of 20 December 2006. A novelty in the impugned version of the provision is that account contents may also be collected in order to obtain information on activities within the meaning of § 3.1 no. 1 of the North Rhine-Westphalia Constitution Protection Act, namely activities which in general terms are targeted against the free democratic fundamental order, the continued existence or the security of the Federation or of a *Land*. According to the reasoning of the Act, this is to make it possible to uncover the channels by means of which domestic terrorist networks, so-called “home-grown networks”, are financed (see *Landtag* document 14/2211, p. 19). 16

4. Equally, only the complainants re 1 complain about the unconstitutionality of § 13 of the North Rhine-Westphalia Constitution Protection Act. This provision empowers the constitution protection authority to process its information in joint files with other security authorities. The provision refers to other federal or *Land* law in respect of the 17

occasion, extent and further requirements as to keeping the files. The complainants re 1 have however not made this other law the subject-matter of their constitutional complaint.

5. Only the complainants re 2 address § 7.2 of the North Rhine-Westphalia Constitution Protection Act. This provision empowers the constitution protection authority to carry out acoustic and optical surveillance of dwellings. It dates from 1994, and was not amended in the context of the revision of the Constitution Protection Act. Thought was given to revising or deleting it, but this was ultimately postponed (see *Landtag* document 14/2211, p. 16). 18

6. Finally, in turn only the complainants re 2 challenge the provisions contained in § 8.4 sentence 2 in conjunction with §§ 10 and 11 of the North Rhine-Westphalia Constitution Protection Act on keeping so-called electronic case files. All in all, these provisions provide that personal data contained in such case files may continue to be stored if the constitution protection authority no longer has any investigative interest in the specific person concerned. This is to ensure the completeness of the electronically maintained case file necessary for electronic document administration. The interests of data protection are accounted for in that the personal data concerned may no longer be searchable, and also may not be used unrestrictedly. 19

7. The following excerpts from the Constitution Protection Act are of interest for the instant proceedings: 20

§ 3 Tasks 21

(1) The task of the constitution protection authority shall be the collection and evaluation of information, in particular of factual and personal information, messages and documents on 22

1. activities targeting the free democratic fundamental order, the continued existence or the security of the Federation or of a *Land* or an unlawful impairment of the exercise of office by the constitutional bodies of the Federation or of a *Land* or of their members, 23

2. activities for a foreign power which endanger security, or for a foreign security service, 24

3. activities which endanger foreign interests of the Federal Republic of Germany by means of the use of force or preparatory acts aimed thereto, 25

4. efforts and activities targeting the ideal of international understanding (Article 9.2 of the Basic Law) or peaceful relations between nations (Article 26 of the Basic Law), 26

within the area of application of the Basic Law, insofar as there exist factual indications of the suspicion of such efforts and activities. 27

… 28

§ 5 Powers

(1) …

(2) In accordance with § 7, the constitution protection authority may apply the following measures to acquire information as intelligence service means:

…

11. secret monitoring and other reconnaissance of the Internet, such as in particular concealed participation in its communication facilities and searching therefor, as well as secret access to information technology systems also involving the deployment of technical means. Insofar as such measures constitute an encroachment on the secrecy of correspondence, post and telecommunication or are equivalent to such encroachment in terms of their nature and grievousness, the latter shall be permissible only under the preconditions of the Act re Article 10 of the Basic Law;

…

(3) Personal data obtained with intelligence service means shall be labelled and transmitted to the persons on whom this information was collected on termination of the measure. Such transmission shall not be necessary if

1. an endangerment of the performance of the task is to be feared from such notification,

2. sources could be placed at risk through provision of the information, or the disclosure of the state of information or the modus operandi of the constitution protection authority is to be feared,

3. notification would endanger public security or would otherwise disadvantage the interests of the Federation or of a *Land*, or

4. the data or the fact of processing must be kept confidential according to a legal provision or because of the prevailing justified interests of a third party,

5. one of the preconditions named at 1-4 still applies after five years subsequent to termination of the measure and will continue to apply in the future with a probability verging on certainty.

…

§ 5a Special powers

(1) The constitution protection authority may in individual cases obtain information free of charge on participants in monetary transactions and on monetary movements and investments from financial institutions, financial service-providers and financial operators if this is necessary in order to perform its tasks in accordance with § 3.1, and factual indications exist of grievous dangers to the protected interests named in § 3.1.

(2) …

(3) Information according to subsections 1 to 2 may only be obtained on request. The request is to be made in writing by the head of the constitution protection department or his or her deputy, and must be reasoned. The Minister of the Interior shall decide on the request. The G 10 Commission (§ 3.1 sentence 1 of the Act on the Implementation of the Act re Article 10 of the Basic Law (*Gesetz über die Ausführung des Gesetzes zu Artikel 10 Grundgesetz – AG G 10 NRW*)) shall be informed without delay of the requests decided on prior to their enforcement. In case of imminent danger, the Minister of the Interior may already order the enforcement of the decision prior to notification of the Commission. The G 10 Commission shall examine the permissibility and necessity of obtaining information ex officio or on the basis of complaints. § 3.5 of the Act on the Implementation of the Act re Article 10 of the Basic Law shall be applied *mutatis mutandis* on proviso that the control power of the Commission covers the entire collection, processing and use of the personal data obtained according to subsections 1 to 2. The Minister of the Interior shall rescind without delay decisions on information which the G 10 Commission declared to be not permissible or not necessary. § 4 of the Act on the Implementation of the Act re Article 10 of the Basic Law shall apply *mutatis mutandis* to the processing of the data collected according to subsections 1 to 2. The request for information and the data transmitted may not be notified to the person concerned or to third parties by the information provider. § 5 of the Act on the Implementation of the Act re Article 10 of the Basic Law shall apply *mutatis mutandis*. 45

… 46

§ 7 Special forms of data collection 47

(1) The constitution protection authority may collect information, in particular personal data, to perform its tasks by enquiring of non-public agencies, and with the means according to § 5.2, if facts justify the presumption that 48

1. information on efforts or activities according to § 3.1, or on the sources necessary to obtain such information, can be obtained by these means, or 49

2. this is necessary to protect the staff, facilities, property and sources of the constitution protection authority against activities which endanger security, or activities of a foreign security service. 50

(2) To avert acute dangers to public safety, in particular a danger to the public or a danger to life (Article 13.4 of the Basic Law), the spoken word not spoken publicly in a dwelling may be secretly monitored or recorded with technical means. Sentence 1 shall apply *mutatis mutandis* to the undercover deployment of technical means to make picture and video recordings. Measures according to sentences 1 and 2 shall be ordered by the head of the constitution protection department or his or her deputy if a judicial ruling cannot be obtained in good time. The judicial ruling shall be obtained subsequently without delay. The Local Court in whose district the constitution protection authority is headquartered shall have jurisdiction. The provisions of the Act 51

on Matters of Non-Contentious Jurisdiction (*Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit*) shall apply accordingly to the proceedings. The information acquired may only be used in accordance with § 4.4 of the Act on the Implementation of the Act re Article 10 of the Basic Law. Technical means within the meaning of sentences 1 and 2 may moreover be used to protect the persons acting in deployment in dwellings insofar as this is indispensable to avert dangers to their life, health or freedom (Article 13.5 of the Basic Law). Measures according to sentence 8 shall be ordered by the head of the constitution protection department or his or her deputy. Apart from the purpose according to sentence 8, the constitution protection authority may only use the data thereby collected to avert danger in the context of its tasks according to § 3.1 nos. 2 to 4, as well as for transmission according to § 4.4 nos. 1 and 2 of the Act on the Implementation of the Act re Article 10 of the Basic Law. Use shall only be permissible if the lawfulness of the measure has been judicially determined prior to this; in case of imminent danger, the judicial ruling shall be subsequently obtained without delay. § 4.6 of the Act on the Implementation of the Act re Article 10 of the Basic Law shall apply *mutatis mutandis*. The fundamental right of the inviolability of the home (Article 13 of the Basic Law) shall be restricted in this respect.

… 52

§ 8 Processing of personal data 53

(1) In the performance its tasks, the constitution protection authority may process personal data in written or electronic files and in files kept on an individual if 54

factual indications exist of the suspicion of efforts and activities according to § 3.1, 55

this is necessary to research and evaluate efforts or activities according to § 3.1, or 56

this is necessary to perform its tasks according to § 3.2. 57

… 58

(4) A record shall be kept of access to personal data in electronic case files. After deletion of the files kept on an individual, personal data stored in electronic case files may not be used for tasks according to § 3.2 or transmitted to other authorities. Such data may not be electronically searchable. 59

… 60

§ 10 Correction, deletion and barring of personal data in files kept on an individual 61

(1) The constitution protection authority shall correct the personal data stored in files if they are incorrect. … 62

(2) The constitution protection authority shall delete the personal data stored in files if its storage was not permissible or if knowledge of it is no longer necessary for the performance of the task. … 63

… 64

§ 11 Correction and barring of personal data in written or electronic files, destruction of files 65

(1) If the constitution protection authority establishes that personal data stored in written or electronic files is incorrect, it shall be corrected. … 66

(2) The constitution protection authority shall bar personal data in written or electronic files if it establishes in an individual case that, without the bar, protected interests of the person concerned would be impaired and that the data is no longer required for its future performance of the task. … 67

(3) The constitution protection authority shall destroy files kept on an individual if these are no longer necessary for the performance of its task and destruction is not opposed by protected interests of the person concerned. … 68

… 69

§ 13 Joint files 70

The constitution protection authority shall be empowered to process personal data in files that are shared with the constitution protection authorities of the Federation and the *Länder*, and with other security authorities, if special federal law or *Land* law provisions regulate the occasion, extent and other requirements relating to data protection. 71

§ 14 Information 72

(1) In response to a written request, the constitution protection authority shall issue to the person making the request free of charge information on the data stored on his or her person, the purpose and the legal basis of the storage. There shall be no right to inspect the files. 73

… 74

§ 17 Transmission of personal data by the constitution protection authority 75

(1) The constitution protection authority may transmit personal data to courts and domestic authorities if this is necessary to perform their tasks, or if the recipient needs the data to perform its tasks in order to protect the free democratic fundamental order or other purposes of public security. … 76

(2) The constitution protection authority may transmit personal data to agencies of the foreign armed forces stationed in Germany insofar as the Federal Republic of Germany is obliged to do so in the context of Article 3 of the additional agreement of 3 August 1959 to the Agreement to supplement the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces with respect to the Foreign Forces stationed in the Federal Republic of Germany (*Zusatzabkommen zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen*) (Federal Law Gazette (*Bundesgesetzblatt – BGBl*) II 1961 pp. 1183 and 1218). 77

(3) The constitution protection authority may transmit personal data to foreign public agencies, as well as to supranational and international agencies, if the transmission is necessary to perform their tasks or to avert a considerable danger to the recipient. … 78

… 79

The Act re Article 10 of the Basic Law, to which § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act refers, contains *inter alia* the following provisions for telecommunication surveillance by constitution protection authorities: 80

§ 1 Subject-matter of the Act 81

(1) 82

1. The constitution protection authorities of the Federation and the *Länder* …, in order to avert dangers threatening the free democratic fundamental order or the continued existence or the security of the Federation or of a *Land*, including the security of the troops of the non-German Parties to the North Atlantic Treaty stationed in the Federal Republic of Germany, 83

2. … 84

shall be empowered to monitor and record telecommunication. … 85

… 86

§ 3 Preconditions 87

(1) Restrictions according to § 1.1 no. 1 may be ordered under the preconditions designated therein if factual indications exist for the suspicion that someone is planning or committing, or has committed 88

1. criminal offences of crimes against peace or of high treason (§§ 80 to 83 of the Criminal Code (*Strafgesetzbuch – StGB*)), 89

2. criminal offences of endangerment of the democratic state based on the rule of law (§§ 84 to 86 and 87 to 89 of the Criminal Code and § 20.1 nos. 1 to 4 of the Associations Act (*Vereinsgesetz*)), 90

3. criminal offences of treason and endangerment of external security (§§ 94 to 96 and 97a to 100a of the Criminal Code), 91

4. criminal offences against national defence (§§ 109e to 109g of the Criminal Code), 92

5. criminal offences against the security of the troops of the non-German Parties to the North Atlantic Treaty stationed in the Federal Republic of Germany (§§ 87, 89, 94 to 96, 98 to 100 and 109e to 109g of the Criminal Code) in conjunction with Article 7 of the Fourth Act Amending Criminal Law (*Viertes Strafrechtsänderungsgesetz*) of 11 June 1957 (Federal Law Gazette. I p. 597) in the version of the Act of 25 June 1968 93

(Federal Law Gazette. I p. 741),

6. criminal offences pursuant to

a) §§ 129a to 130 of the Criminal Code, as well as

b) §§ 211, 212, 239a, 239b, 306 to 306c, 308.1 to 308.3, § 315.3, § 316b.3 and § 316c.1 and 316c.3 of the Criminal Code, insofar as these target the free democratic fundamental order, the continued existence or the security of the Federation or of a *Land*, or

7. criminal offences pursuant to § 95.1 no. 8 of the Residence Act (*Aufenthaltsgesetz*).

The same shall apply if factual indications of the suspicion exist that someone is a member of an association the purpose or activities of which are intended to commit criminal offences targeting the free democratic fundamental order, the continued existence or the security of the Federation or of a *Land*.

(2) The order shall only be permissible if the researching of the facts by other means would be devoid of prospects or considerably more difficult. It may only target the suspect or persons of whom it can be presumed as a result of certain facts that they accept or pass on messages intended for the suspect or originating from him or her, or that the suspect uses their connection. Measures relating to postal items shall only be permissible with regard to those postal items with regard to which facts justify the presumption that they originate from the person whom the order targets or are intended for him or her. Parliamentary mail from members of the German *Bundestag* and the Parliaments of the *Länder* may not be included in a measure targeting a third party.

§ 4 Review, labelling and deletion obligations, transmissions, limitation principle

(1) The collecting agency shall examine without delay and then at intervals of at most six months whether the collected personal data is necessary in the context of its tasks for the purposes designated in § 1.1 no. 1, on their own or together with data that is already available. Insofar as the data is not necessary for these purposes and is not needed for transmission to other agencies, it shall be deleted without delay under the supervision of an official who has the qualification to hold judicial office. …

…

§ 9 Request

(1) Restrictive measures according to this statute may only be ordered on request.

…

§ 10 Order

(1) The authority competent to order restrictive measures with regard to requests from the constitution protection authorities of the *Länder* shall be the competent high-

est *Land* authority, or otherwise a Federal Ministry commissioned by the Federal Chancellor.

…

§§ 4 and 5 of the North Rhine-Westphalian Act on the Implementation of the Act re Article 10 of the Basic Law (*nordrhein-westfälisches Gesetz über die Ausführung des Gesetzes zu Artikel 10 Grundgesetz*) (below: Act on the Implementation of the Act re Article 10 of the Basic Law – *AG G 10 NRW*), referred to in § 5a.3 of the North Rhine-Westphalia Constitution Protection Act, read as follows in excerpts:

§ 4 Review, labelling and deletion obligations, transmissions, limitation principle

(1) The collecting agency shall examine without delay, and then at intervals of at most six months, whether the collected personal data is necessary in the context of its tasks for the purposes designated in § 1.1 no. 1 of the Act re Article 10 of the Basic Law, on its own or together with data that is already available. Insofar as the data is not necessary for these purposes and is not needed for transmission to other agencies, it shall be deleted without delay under the supervision of an official who has the qualification to hold judicial office. …

…

§ 5 Control of transmission to persons concerned by the G 10 Commission

(1) Restrictive measures shall be notified to persons concerned by the Minister of the Interior after their cessation if a risk to the purpose of the restriction can be ruled out. …

…

1. The complainant re 1a is a journalist and writes primarily for an online publication. In the context of her work, she also visits Internet sites which are operated by anti-constitutional persons and organisations. She is also committed to data protection matters, and together with others operates the website www.stop1984.com. In connection with this site it is possible to participate in so-called chats. This possibility is also used by right-wing extremists. The complainant re 1a stores information on these individuals on the hard disk of her computer, which she uses for both private and work purposes.

The complainant re 1b is an active member of the North Rhine-Westphalian *Land* association of the party DIE LINKE, which is being observed by the North Rhine-Westphalian constitution protection authority. He also uses his computer, which is connected to the Internet, for his political activities. Like the complainant re 1a, he also uses the Internet for private communication and to transact payments via his current account.

The complainants re 2a and 2b are partners in a law firm. The complainant re 2a assists as a lawyer asylum-seekers amongst others. One of these was a leading mem-

ber of the Kurdistan Workers' Party PKK, which is being observed by the North Rhine-Westphalian constitution protection authority. He uses computer networks which are connected to the Internet, both in his dwelling and in the premises of the law firm. The office network is also used by the complainant re 2b, as well as by the complainant re 2c, who is employed in the office as a freelancer.

2. Insofar as the constitutional complaints target § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act, the complainants complain of a violation of Article 2.1 in conjunction with Article 1.1, Article 10.1 and Article 13.1 of the Basic Law. 119

[The complainants submit the following:] Insofar as the provision provides for participation in communication facilities of the Internet, it regulates an encroachment on the secrecy of telecommunication. An encroachment on Article 13 of the Basic Law is said to be constituted by the secret access to information technology systems that is further provided by the provision if the access computer is located in a dwelling. According to the complainants, it is relevant in this respect that personal conduct modes enjoy special protection particularly by virtue of their realisation in the spatially separate dwelling. Such measures could also encroach on the general right of personality and on the secrecy of telecommunication. 120

Insofar as measures according to § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act are to be regarded as an encroachment on Article 13 of the Basic Law, the provision is already said to be unconstitutional because it allegedly meets none of the special barrier reservations of Article 13.2 to 13.7 of the Basic Law. Also, the principle of specifying [the fundamental right which is restricted] contained in Article 19.1 sentence 2 of the Basic Law is said to not have been complied with. 121

§ 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act is additionally said to violate the principle of the clarity of provisions. The reference to the Act re Article 10 of the Basic Law contained in sentence 2 of the provision is said to be sufficiently determined neither in its preconditions, nor in its range. Further, there are said to be no sufficient normative precautions to protect individual development in the core area of private life. Such precautions are said to be required since privately used computers in particular are frequently used today to process data with highly personal contents. Finally, the principle of proportionality is said not to have been complied with. The statutory encroachment threshold is said to have been placed too low. What is more, there is said to be a lack of procedural precautions, such as a requirement of a judicial order, to protect the person concerned. The data collected could also be diverted from its intended use to a too great degree or transmitted to other authorities. 122

3. The complainants further complain that § 5.3 of the North Rhine-Westphalia Constitution Protection Act allegedly violates the legal protection guarantee contained in Article 19.4 of the Basic Law, as well as the substantive fundamental rights which were encroached upon by measures according to § 5.2 of the North Rhine-Westphalia Constitution Protection Act. Sentence 2 of the provision is said to provide 123

excessively broad exceptions to the obligation of notification demanded by the fundamental rights concerned, thus largely rendering it ineffective.

4. The complainants re 1 are of the view that § 5a.1 of the North Rhine-Westphalia Constitution Protection Act violates the right to informational self-determination. The provision is said to facilitate the collection of account contents under insufficiently stringent preconditions, and is hence said to be disproportionate. 124

§ 13 of the North Rhine-Westphalia Constitution Protection Act is said to violate the principle of separation between secret services and police authorities, which is regarded as an expression of the principle of the rule of law in conjunction with the right to informational self-determination. 125

5. The complainants re 2 submit that § 7.2 of the North Rhine-Westphalia Constitution Protection Act allegedly violates Article 13.1 of the Basic Law. The provision is said not to comply with the requirements which the Federal Constitutional Court (*Bundesverfassungsgericht*) stipulated in its judgment on acoustic monitoring of dwellings in criminal procedure. 126

§ 8.4 sentence 2 of the North Rhine-Westphalia Constitution Protection Act is said to violate the right to informational self-determination since it does not contain a regulation on the deletion of personal data in electronic case files. The provision is hence alleged to make impermissible stockpiling of data possible. 127

Insofar as data is said to be concerned which had been obtained by a measure according to § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act, finally, the transmission provision contained in § 17.1 of the North Rhine-Westphalia Constitution Protection Act is also said to be unconstitutional. It is said to violate the imperatives of the purpose limitation principle of the clarity of provisions and of proportionality. 128

II.

Written statements on the constitutional complaints have been submitted by: the Federal Government, the *Land* Government and the *Landtag* (state parliament) of North Rhine-Westphalia, the Saxon State Government, the Federal Administrative Court (*Bundesverwaltungsgericht*), the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) and the *Land* Commissioner for Data Protection and Freedom of Information (*Landesbeauftragte für Datenschutz und Informationsfreiheit*) of North Rhine-Westphalia. The parliamentary groups of the SPD and Alliance 90/The Greens in the North Rhine-Westphalian *Landtag* have submitted a legal expert report commissioned by them. The Senate has also commissioned expert written statements from Andreas Bogk, Dirk Fox, Professor Dr. Felix Freiling, Professor Dr. Andreas Pfitzmann and Professor Dr. Ulrich Sieber. 129

1. The Federal Government discusses in general terms without directly referring to 130

the impugned provisions the constitutional questions of secret access to information technology systems using technical means:

It is said to be necessary to distinguish between such measures and the surveillance of telecommunication falling under Article 10 of the Basic Law. It has been presumed in the case of the “online searches” that have been carried out individually in the past by the Federal Office for the Protection of the Constitution that the sole fundamental right standard is Article 2.1 in conjunction with Article 1.1 of the Basic Law. However, Article 13.1 of the Basic Law is increasingly occurring as a possibly relevant standard for “online searches”. The technical possibility of the repeated incursion into or longer-term connection to a computer is said to make the “online search” more akin to surveillance. At least in the perception of the persons concerned, a very comprehensive part of the private sphere which had previously been spread among the rooms of a dwelling can now be concentrated in the computer. 131

Access is said to require special procedural safeguards as a qualified means of constitution protection. The protection of the core area of private life is to be maintained, even if it cannot already be secured on copying and transferring the information considered as relevant by the software on the basis of certain search parameters, but only when subsequently inspecting the files on the authority’s computer. In view of the similarity to measures of house searches and monitoring of dwellings, it must be considered to place access under the reservation of a judicial order. In principle, an obligation to notify should be provided for. Moreover, “online searches” should be subject to stringent requirements as to proportionality. In view of its encroachment intensity, such a measure can only be the *ultima ratio* for a constitution protection authority. 132

2. The Government of the *Land* North Rhine-Westphalia considers the constitutional complaints to be inadmissible, but at any rate to be unfounded: 133

According to the Government of the *Land* North Rhine-Westphalia, the measures provided for in § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act do not bring about any encroachment on Article 13 of the Basic Law. This fundamental right is said to apply only if a state measure shows a concrete spatial reference, if in other words spatial boundaries are overcome. This is said not to be the case here. Measures of reconnaissance of the Internet, such as the surveillance of e-mail traffic or of Internet telephony, are however said to be measured against the standard of Article 10 of the Basic Law. Moreover, the right to informational self-determination is said to be relevant. 134

§ 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act is said to satisfy the principle of the clarity of provisions. The provision is said to have been worded in a manner that is open to developments with regard to possible technical novelties. The provision is further said to respect the core area of private life. The required protection of the core area is said to be ensured by § 4.1 of the Act re Article 10 of the Basic Law, to which reference is said to be made. The impugned provision is said finally also to be proportionate. The scope of action for the constitution protection authority 135

has to take account of the increasing shift in communication, and in particular also of anti-constitutional activities, to the Internet. Access to individual computers is said to be necessary because it is technically possible to send communication contents such that access during transmission is impossible. § 7.1 of the North Rhine-Westphalia Constitution Protection Act is said to contain an adequate encroachment threshold in this regard. Further substantive criteria and procedural precautions are said to emerge from § 3 of the Act re Article 10 of the Basic Law in particular. According to the Government of the *Land* North Rhine-Westphalia, one should expect the number of cases of access to information technology systems to be fewer than ten per year.

The regulation as to the obligations of labelling and notification in § 5.3 of the North Rhine-Westphalia Constitution Protection Act is said to be equally constitutionally unobjectionable. It is said to be not § 5.3 of the North Rhine-Westphalia Constitution Protection Act which applies to measures of Internet reconnaissance according to § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act, but in fact § 12 of the Act re Article 10 of the Basic Law. 136

The empowerment contained in § 5a.1 of the North Rhine-Westphalia Constitution Protection Act to retrieve account content data is said to be also constitutional. The phenomenon of so-called home-grown networks pursuing the goal of domestic attacks is said to constitute a new type of considerable risk. The empowerment could help in the reconnaissance of personal interconnections and channels for funding, such as in arms procurement, and of the donors of militant groups. 137

3. The North Rhine-Westphalian *Landtag* also considers the constitutional complaints to be unfounded: 138

The expansion of international terrorism is said to create a new type of threat which forces the state to restrict fundamental rights in the interest of effective anti-terror activities. The state based on the rule of law must carefully refine the traditional set of legal tools in order to meet new challenges. In particular, the information technology actionability of the security authorities has to be adjusted to the new circumstances. Modern communication technologies are being used in the commission and preparation of a wide range of criminal offences, and hence are said to be helping to make crime more effective. 139

It is said to be true that intensive encroachments on fundamental rights are not permissible in classical police law until a certain degree of suspicion or danger exists. This is however said to be based on a field of activities of authorities which is fundamentally different from the activities of the constitution protection authorities. As a rule, no direct sanctions or consequences for the persons concerned are linked with obtaining structural preliminary information in order to reconnoitre terrorist activities. 140

Article 13 of the Basic Law is said to not be affected by measures according to § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act. Access to stored data is said not to aim at overcoming the spatial delimitation of a dwelling. Also, no 141

events taking place in the dwelling are intended to be monitored. By contrast, an encroachment on Article 10 of the Basic Law might take place in an individual case. The provision however is said to meet the constitutional requirements as to the justification of the encroachment.

The exceptions from the obligation to notify laid down in § 5.3 sentence 2 of the North Rhine-Westphalia Constitution Protection Act are also said to be compatible with the Basic Law. 142

4. The Saxon State Government states that communication within Islamist and Islamist-terrorist groups is largely taking place via the Internet. Left-wing autonomists are also said to be using the Internet and mobile telephones offering protected communication. Access via classical intelligence service means has become impossible in some cases, given the increased use of information technology systems by persons who are being monitored. 143

§ 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act is said not to grant powers to perform encroachments on Article 10.1 or Article 13.1 of the Basic Law. Apart from this, the provision is said to be sufficiently precise and proportionate in other respects. The core area of private life is however said not to be affected since the citizen does not depend on a personal computer for highly personal communication. § 5.3, § 5a.1 and § 13 of the North Rhine-Westphalia Constitution Protection Act are also said to be in compliance with the Basic Law. 144

5. The Federal Administrative Court expresses constitutional reservations against the empowerment to secretly access information technology systems contained in § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act. There are said to be weighty arguments both for and against the application of Article 13 of the Basic Law. At all events, regulated access is said to encroach on the right to informational self-determination. It is said to appear doubtful whether this encroachment is proportionate. It is said to suggest itself in view of the weight of the encroachment on fundamental rights to make an “online search” contingent on a concrete danger to certain legal interests. The statute is said not to contain any precautions to protect the core area of private life. 145

6. The Federal Commissioner for Data Protection and Freedom of Information and the *Land* Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia consider the impugned provisions to be unconstitutional. Their statements on this largely concur with the complainants’ line of argument in their content-related argumentation and in their conclusions. 146

7. The parliamentary groups of the SPD and Alliance 90/The Greens in the North Rhine-Westphalian *Landtag* have submitted a legal expert report that commissioned by them. This report concludes that the impugned provisions are compatible neither with the Basic Law nor with the North Rhine-Westphalian *Land* Constitution. 147

8. The experts Andreas Bogk, Dirk Fox, Professor Dr. Felix Freiling and Professor 148

Dr. Andreas Pfitzmann have in particular made statements on the technical questions related to secret access to information technology systems; Professor Dr. Ulrich Sieber also made a statement on questions related to comparative law and on possible requirements as to the lawfulness of the measures discussed here.

III.

Statements were made in the oral hearing by: the complainants, the Federal Government, the Federal Criminal Police Office, the Federal Office for the Protection of the Constitution, the Federal Office for Security in Information Technology (*Bundesamt für Sicherheit in der Kommunikationstechnik*), the *Land* Government and the *Landtag* of North Rhine-Westphalia, the North Rhine-Westphalian *Land* Office for the Protection of the Constitution, the Federal Commissioner for Data Protection and Freedom of Information, the *Land* Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia, and as experts Andreas Bogk, Dirk Fox, Professor Dr. Felix Freiling, Professor Dr. Andreas Pfitzmann and Professor Dr. Ulrich Sieber. 149

B.

The constitutional complaints are only partly admissible. 150

I.

Insofar as the constitutional complaints address § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act, there are no objections as to their admissibility. 151

II.

As to the complaint of the unconstitutionality of § 5.3 of the North Rhine-Westphalia Constitution Protection Act lodged by all complainants, the constitutional complaints are only admissible insofar as they relate to the notification subsequent to a measure according to § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act. In other respects, the reasoning of the constitutional complaints does not meet the requirements of § 23.1 sentence 2 and § 92 of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz – BVerfGG*). Accordingly, a constitutional complaint is to be reasoned with sufficient grounds. The complainant must explain the constitutional requirements with which the impugned measure collides. In order to do so, he or she must indicate to what degree it is alleged to violate the designated fundamental rights (see Decisions of the Federal Constitutional Court (*Entscheidungen des Bundesverfassungsgerichts* – BVerfGE) 99, 84 (87); 108, 370 (386)). 152

This is not the case here insofar as the complainants complain in general terms that the regulation on subsequent notification of intelligence service measures within the meaning of § 5.2 of the North Rhine-Westphalia Constitution Protection Act does not 153

meet the constitutional requirements. To what degree the Basic Law requires notification of the person concerned by a secret informational measure carried out by the state depends decisively amongst other things on whether and with what intensity this measure encroaches on fundamental rights of the person concerned (see Federal Constitutional Court – BVerfG, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift – NJW* 2007, p. 2464 (2473)). § 5.2 of the North Rhine-Westphalia Constitution Protection Act provides for a large number of different measures which differ considerably from one another as to the quality and intensity of their encroachment. In view of this, the complainants could have and should have shown according to which of these measures notification is necessary in their view, and to what degree the exceptions from the obligation of notification regulated in § 5.3 sentence 2 of the North Rhine-Westphalia Constitution Protection Act are inappropriate in view of the gravity of the respective encroachment on fundamental rights. Such statements can however only be found to a sufficient degree in the constitutional complaints with regard to measures according to § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act.

III.

154 The constitutional complaint of the complainants re 2 is also permissible insofar as it addresses § 17 of the North Rhine-Westphalia Constitution Protection Act. In this sense, the complaint deadline contained in § 93.3 of the Federal Constitutional Court Act has been met. By virtue of the entry into force of § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act, the area of application of the general transmission provision contained in § 17 of the North Rhine-Westphalia Constitution Protection Act was made to cover the newly regulated measures, and hence partly expanded. This constitutes a new fundamental rights-related cause of complaint for which the complaint deadline is re- started (see BVerfGE 45, 104 (119); 78, 350 (356); 100, 313 (356)). The complaint of the complainants re 2 is restricted to this new cause of complaint.

IV.

155 The constitutional complaint of the complainant re 1b is also admissible insofar as it addresses § 5a.1 of the North Rhine-Westphalia Constitution Protection Act. In particular, the complaint deadline has been met. The complaint of the complainant re 1b is restricted to the expansion of the area of application of the provision in the course of the revision of the Constitution Protection Act.

156 The constitutional complaint of the complainant re 1a is, by contrast, inadmissible with regard to § 5a.1 of the North Rhine-Westphalia Constitution Protection Act since she has not shown that she is personally and presently concerned by the impugned provision. To this end, she would have had to submit that with some probability her fundamental rights are affected by the measures based on the impugned legal provisions (see BVerfGE 67, 157 (169-170); 100, 313 (354); 109, 279 (307-308)). This is

not evident here. The complainant re 1a has stated nothing from which only the most distant probability emerges that her account content data could be of interest to the constitution protection authority. According to the factual preconditions of § 5a.1 of the North Rhine-Westphalia Constitution Protection Act and the nature of the measures regulated, one may also not presume for practically all and sundry that they might be affected (see re such cases BVerfGE 109, 279 (308); 113, 348 (363)).

V.

157 The complaint deadline contained in § 93.3 of the Federal Constitutional Court Act has not been met insofar as the constitutional complaint of the complainants re 2 addresses § 7.2 of the North Rhine-Westphalia Constitution Protection Act. This provision entered into force back in 1994. It is without interest here whether the Parliament handing down the revision of the Constitution Protection Act re-included § 7.2 of the North Rhine-Westphalia Constitution Protection Act in its intention, since the complaint deadline is not re-started thereby (see BVerfGE 11, 255 (259-260); 18, 1 (9); 43, 108 (116); 80, 137 (149)).

158 The complainants re 2 are not deprived of the possibility to claim the unconstitutionality of the impugned provision by virtue of the inadmissibility of the constitutional complaint with regard to this item (see on this Federal Constitutional Court, Order of the 1st Chamber of the First Senate of 21 November 1996 – 1 BvR 1862/96 –, *Neue Juristische Wochenschrift* 1997, p. 650). If the complainants re 2 fear being affected by measures according to § 7.2 of the North Rhine-Westphalia Constitution Protection Act, they may obtain legal protection from the administrative courts against this. Preliminary and precautionary legal protection can also in principle be granted in such instances. The circumstance that a legitimate interest in the ruling and the probability of a burdening measure must be sufficiently shown for this does not rule out the fundamental availability of recourse to the legal protection of the non-constitutional courts. In the interest of effective fundamental rights protection, the requirements placed on the legitimate interest in a ruling may not be excessive in the proceedings before the non-constitutional courts (see in general terms on this BVerfGE 110, 77 (88)).

VI.

159 The constitutional complaint of the complainants re 2 is also inadmissible insofar as it addresses the provisions of § 8.4 sentence 2 in conjunction with §§ 10 and 11 of the North Rhine-Westphalia Constitution Protection Act on management of personal data in electronic case files. The principle of the subsidiarity of the constitutional complaint has not been met as to these provisions.

160 According to the principle of subsidiarity, the constitutional complaint of a subject of fundamental rights affected by the impugned legal provision is inadmissible if he or she can obtain legal protection in an acceptable manner by taking recourse to the

courts (see BVerfGE 72, 39 (43-44); 90, 128 (136-137)). This is intended to prevent the Federal Constitutional Court from handing down high-impact rulings on an insecure factual and legal basis (see BVerfGE 79, 1 (20); 97, 157 (165)).

Accordingly, the complainants re 2 must first of all take recourse to the non-constitutional courts to obtain legal protection against the provisions of the Constitution Protection Act on management of personal data which is stored in electronic case files. 161

The complainants re 2 address their complaint against the storage of personal data that is no longer needed, which in their view is provided by the Constitution Protection Act. How extensively the statute rules out the deletion of such data however initially requires clarification under non-constitutional law by the authorities and by the non-constitutional courts. The wording of § 10 of the North Rhine-Westphalia Constitution Protection Act at any rate does not rule out applying the existing deletion rules in this provision also to data which is contained in electronic case files. Moreover, the statute does not contain any explicit provisions on the management of electronic case files that are no longer needed, so that the legal situation is also unclear in this respect. 162

The complainants re 2 can be expected to have the situation under non-constitutional law clarified by the non-constitutional courts which have jurisdiction therefor. In particular, they are not prevented de facto from taking recourse to the courts simply because they were not able to obtain knowledge of the data storage relating to them. In contradistinction to the view held by the complainants re 2, it does not necessarily emerge from the wording of § 14.1 of the North Rhine-Westphalia Constitution Protection Act that personal data kept in electronic case files is not covered from the outset by the claim to information regulated in this provision, so that one may not rule out that information must be provided in this respect. What is more, by the complaint addressed against § 8.4 sentence 2 of the North Rhine-Westphalia Constitution Protection Act, the complainants re 2 do not intend to avert a specific act of encroachment on fundamental rights which could only to a limited degree be remedied by subsequent legal protection. Rather, they wish to claim substantive deletion rights which they can enforce in the proceedings before the non-constitutional courts. 163

VII.

Insofar as the complainants re 1 complain of the alleged unconstitutionality of § 13 of the North Rhine-Westphalia Constitution Protection Act, their constitutional complaint is inadmissible because they are not directly affected. § 13 of the North Rhine-Westphalia Constitution Protection Act permits the constitution protection authority to place data in joint files which are maintained according to federal or *Land* law. Only on the basis of these other provisions can measures be effected which could be regarded as an encroachment on fundamental rights. The opening provision of § 13 of the North Rhine-Westphalia Constitution Protection Act, which is rendered ineffective 164

without the rules on maintaining files referred to, is irrelevant per se in terms of the fundamental rights. The constitutional complaint of the complainants re 1 is however not addressed against provisions that are referred to, such as the provisions of the Anti-Terror File Act (*Antiterrordateigesetz*) of 22 December 2006 (Federal Law Gazette I, p. 3409).

C.

Insofar as they are admissible, the constitutional complaints are largely well founded. § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act is unconstitutional and null and void in the second alternative listed there (I.). The same applies to the first alternative of this provision (II.). As a result of the nullity, the complaints addressed against § 5.3 and § 17 of the North Rhine-Westphalia Constitution Protection Act are disposed of (III.). By contrast, there are no constitutional objections (IV.) against § 5a.1 of the North Rhine-Westphalia Constitution Protection Act. 165

I.

§ 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act, which regulates secret access to information technology systems, violates the general right of personality (Article 2.1 in conjunction with Article 1.1 of the Basic Law) in its particular manifestation as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems. 166

This manifestation of the general right of personality protects against encroachment on information technology systems, insofar as the protection is not guaranteed by other fundamental rights, such as in particular Article 10 or Article 13 of the Basic Law, as well as by the right to informational self-determination (1). In the instant case, the encroachments are not constitutionally justified: § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act does not comply with the principle of the clarity of provisions (2 a), the requirements of the principle of proportionality are not met (2 b) and the provision does not contain any sufficient precautions to protect the core area of private life (2 c). The impugned provision is null and void (2 d). There is no need for an additional review against other fundamental rights (2 e). 167

1. § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act grants powers to encroach on the general right of personality in its special manifestation as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems; it enters the field besides the other concrete forms of this fundamental right, such as the right to informational self-determination, as well as the guarantees of freedom contained in Article 10 and Article 13 of the Basic Law, insofar as these do not guarantee any or sufficient protection. 168

a) The general right of personality guarantees elements of the personality which are 169

not the subject-matter of the special guarantees of freedom contained in the Basic Law, but which are not inferior to these in their constituting significance for the personality (see BVerfGE 99, 185 (193); 114, 339 (346)). Such a loophole-closing guarantee is needed in particular in order to counter new types of endangerment which may occur in the course of scientific and technical progress or changed circumstances (see BVerfGE 54, 148 (153); 65, 1 (41); Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2465)). The assignment of a concrete legal protection claim regarding the various aspects of the right of personality conforms above all to the type of danger to the personality (see BVerfGE 101, 361 (380); 106, 28 (39)).

b) The use of information technology has taken on a significance for the personality and the development of the individual which could not have been predicted. Modern information technology provides the individual with new possibilities, whilst at the same time entailing new types of endangerment of personality. 170

aa) Recent developments in information technology have led to a situation in which information technology systems are omnipresent and their use is central to the lives of many citizens. 171

This applies first and foremost to personal computers, which can now be found in a large majority of households in the Federal Republic (see Federal Statistical Office, *Statistisches Jahrbuch* 2007, p. 113). The performance of such computers has increased, as has the capacity of their internal memories and of the storage media connected with them. Today's personal computers can be used for a large number of different purposes, such as for the comprehensive administration and archiving of an individual's personal and business matters, as a digital library or in many ways as an entertainment appliance. Accordingly, the significance of personal computers for the development of personality has increased considerably. 172

The relevance of information technology for the life of the individual is not limited to a greater spread and performance of personal computers. Additionally, many objects which are used on an everyday basis by large sections of the population involve information technology components. This is increasingly the case for instance with telecommunication or electronic appliances which are contained in dwellings or motor vehicles. 173

bb) The performance of information technology systems and their significance for the development of personality increase further if such systems are networked with one another. This is increasingly becoming the norm, in particular because of the increased use of the Internet by large groups of the population. 174

The networking of information technology systems facilitates in general terms the distribution of tasks among these systems and increases the total computing performance. Thus, for instance, data provided by individual networked systems can be evaluated and the systems made to react in a certain manner. The scope of the func- 175

tion of the individual system can be simultaneously expanded by these means.

In particular the Internet, as a complex combination of computer networks, not only provides users of a computer that is connected to it with access to a practically limitless mass of information which is ready for retrieval from other network computers. It also provides them with many new types of communication services, allowing them to establish and maintain active social contacts. Technical convergence effects also lead to traditional forms of telecommunication being shifted to the Internet to a considerable extent (see for instance on speech telephony Katko, *Computer und Recht – CR* 2005, p. 189). 176

cc) The increasing spread of networked information technology systems entails for the individual new endangerments of personality, in addition to new possibilities for the development of the personality. 177

(1) Such endangerments emerge from the fact that complex information technology systems such as personal computers open up a broad spectrum of use possibilities, all of which are associated with the creation, processing and storage of data. This is not only data which computer users create or store deliberately. In the context of the data processing process, information technology systems also create by themselves large quantities of further data which can be evaluated as to the user's conduct and characteristics in the same way as data stored by the user. As a consequence, a large amount of data can be accessed in the working memory and on the storage media of such systems relating to the personal circumstances, social contacts and activities of the user. If this data is collected and evaluated by third parties, this can be highly illuminating as to the personality of the user, and may even make it possible to form a profile (see on the personality endangerments resulting from such conclusions BVerfGE 65, 1 (42)). 178

(2) These risks are exacerbated in a variety of ways in a networked system, in particular one which is connected to the Internet. Firstly, the expansion of the facilities offered by networking leads to a situation in which an even greater number and diversity of data is created, processed and stored in comparison to a stand-alone system. This includes communication contents, as well as data relating to network communication. Wide-ranging knowledge of the personality of the user can be obtained by storing and evaluating such data on the conduct of the users in the network. 179

Above all, however, the networking of the system opens to third parties a technical access facility which can be used in order to spy on or manipulate data kept on the system. The individual cannot detect such access at all in some cases, or at least can only prevent it to a restricted degree. Information technology systems have now reached such a degree of complexity that effective social or technical self-protection leads to considerable difficulties and may be beyond the ability of at least the average user. Technical self-protection may also entail considerable effort or result in the loss of the functionality of the protected system. Many possibilities of self-protection – such as encryption or the concealment of sensitive data – are also largely ineffective 180

if third parties have been able to infiltrate the system on which the data has been stored. Finally, it is not possible in view of the speed of the development of information technology to reliably forecast the technical means which users may have to protect themselves in future.

c) A need for protection that is relevant from the fundamental rights perspective emerges from the significance of the use of information technology systems for the development of the personality and from endangerments of the personality linked with this use. The individual relies on the state respecting the expectations of the integrity and confidentiality of such systems which are justified with regard to the unhindered development of the personality. The fundamental rights guarantees contained in Article 10 and Article 13 of the Basic Law, like those manifestations of the general right of personality previously developed in the case-law of the Federal Constitutional Court, do not adequately take account of the need for protection arising as a consequence of the development of information technology. 181

aa) The guarantee of the secrecy of telecommunication according to Article 10.1 of the Basic Law protects the non-physical transmission of information to individual recipients with the aid of telecommunication traffic (see BVerfGE 67, 157 (172); 106, 28 (35-36)), but not the confidentiality and integrity of information technology systems. 182

(1) The protection of Article 10.1 of the Basic Law covers telecommunication, regardless of the method of transmission (cable or broadcast, analogue or digital transmission) and the form of expression (speech, pictures, sound, symbols or other data) which are used (see BVerfGE 106, 28 (36); 115, 166 (182)). The scope of protection of the secrecy of telecommunication accordingly also covers the communication services of the Internet (see re e-mails BVerfGE 113, 348 (383)). What is more, not only the contents of the telecommunication are protected against knowledge being obtained of them, but also their circumstances. This includes in particular whether, when and how frequently telecommunication traffic has taken place or has been attempted between which persons or telecommunication facilities (see BVerfGE 67, 157 (172); 85, 386 (396); 100, 313 (358); 107, 299 (312-313)). In this context, the confidentiality of telecommunication encounters both old and new endangerments of personality emerging from the increased significance of information technology for the development of the individual. 183

Insofar as an empowerment is restricted to a state measure by means of which the contents and circumstances of the ongoing telecommunication are collected in the computer network, or the data related thereto is evaluated, the encroachment is to be measured against Article 10.1 of the Basic Law alone. The scope of protection of this fundamental right is affected here regardless of whether in technical terms the measure targets the transmission channel or the terminal used for telecommunication (see BVerfGE 106, 28 (37-38); 115, 166 (186-187)). This also applies in principle if the terminal is a networked complex information technology system the use of which for telecommunication is only one among several types of use. 184

(2) The fundamental rights protection provided by Article 10.1 of the Basic Law however does not cover the contents and circumstances of the telecommunication stored subsequent to completion of the communication in the sphere of a subscriber, insofar as he or she can take their own protective precautions against secret data access. The specific dangers of spatially distanced communication which are to be averted by secrecy of telecommunication do not then continue to apply to such data (see BVerfGE 115, 166 (183 et seq.)). 185

(3) The protection effected by secrecy of telecommunication likewise does not apply if a state agency monitors the use of an information technology system as such or searches the storage media of the system. As to the collection of contents or circumstances outside the ongoing telecommunication, an encroachment on Article 10.1 of the Basic Law does not apply even if a telecommunication connection is used for transmission of the data collected to the evaluating authority, as is the case for instance with online access to stored data (see Germann, *Gefahrenabwehr und Strafverfolgung im Internet*, 2000, p. 497; Rux, *Juristenzeitung* 2007, p. 285 (292)). 186

(4) Insofar as the secret access to an information technology system serves to collect data also where Article 10.1 of the Basic Law does not provide protection against access, a loophole in protection exists which is to be closed by the general right of personality in its manifestation as a protection of the confidentiality and integrity of information technology systems. 187

If a complex information technology system is technically infiltrated in order to perform telecommunication surveillance (“source telecommunication surveillance”), the infiltration overcomes the critical hurdle to spying on the system as a whole. The endangerment thereby brought about goes far beyond what is entailed by the mere surveillance of ongoing telecommunication. In particular, the data stored on personal computers which does not relate to the use of the system for telecommunication can also be obtained. For instance, the conduct in using a personal computer for personal purposes, the frequency of accessing certain services, in particular also the contents of files created or – insofar as the infiltrated information technology system also controls appliances in households – the conduct in the personal dwelling can be discovered. 188

According to information from the experts heard in the oral hearing, moreover, it may happen that, data is collected following infiltration which is unrelated to the ongoing telecommunication, even if this is not intended. As a result – and in contradistinction to what is usually the case with traditional network-based telecommunication surveillance – there is always a risk for the person concerned that further personal information is collected over and above the contents and circumstances of telecommunication. The specific endangerments of personality which this brings about cannot be countered or cannot be sufficiently countered by Article 10.1 of the Basic Law. 189

Article 10.1 of the Basic Law is by contrast the sole fundamental right-related standard for the evaluation of an empowerment to engage in “source telecommunication 190

surveillance" if the surveillance is restricted exclusively to data emanating from an ongoing telecommunication process. This must be ensured by technical precautions and legal instructions.

bb) Also the guarantee of the inviolability of the home granted by Article 13.1 of the Basic Law guarantees an elementary space to the individual with regard to his or her human dignity, as well as in the interest of the development of his or her personality, which may be encroached upon only under the special preconditions of Article 13.2 to 13.7 of the Basic Law, but leaves loopholes as regards access to information technology systems. 191

The interests protected by this fundamental right are constituted by the spatial sphere in which private life takes place (see BVerfGE 89, 1 (12); 103, 142 (150-151)). In addition to private dwellings, company and business premises are also within the scope of protection of Article 13 of the Basic Law (see BVerfGE 32, 54 (69 et seq.); 44, 353 (371); 76, 83 (88); 96, 44 (51)). The fundamental rights protection is not restricted here to the prevention of physical penetration of the dwelling. Measures by means of which state agencies use special aids to obtain an impression of events within the dwelling which are removed from the natural perception from outside the protected area are also to be regarded as an encroachment on Article 13 of the Basic Law. This includes not only acoustic or optical monitoring of dwellings (see BVerfGE 109, 279 (309, 327)), but also for instance the measurement of electromagnetic radiation with which the use of an information technology system in the dwelling can be monitored. This can also concern a system which operates offline. 192

Over and above this, a state measure which is connected to secret technical access to an information technology system may be measured against Article 13.1 of the Basic Law, for instance if and insofar as staff of the investigation authority seek access to premises that are protected as a dwelling in order to physically manipulate an information technology system there. A further case of the application of Article 13.1 of the Basic Law is the infiltration of an information technology system in a dwelling in order to monitor certain events within the dwelling by using it, for instance by using peripherals connected to the system, such as a microphone or a camera. 193

Article 13.1 of the Basic Law does not however confer on the individual any across-the-board protection regardless of the access modalities against the infiltration of his or her information technology system, even if this system is located in a dwelling (see for instance Beulke/Meininghaus, *Der Strafverteidiger – StV* 2007, p. 63 (64); Gercke, *Computer und Recht* 2007, p. 245 (250); Schlegel, *Goltdammer's Archiv für Strafrecht* 2007, p. 648 (654 et seq.); other view for instance Buermeyer, *Höchstrichterliche Rechtsprechung im Strafrecht* 2007, p. 392 (395 et seq.); Rux, *Juristenzeitung* 2007, p. 285 (292 et seq.); Schaar/Landwehr, *Kommunikation & Recht* 2007, p. 202 (204)). The encroachment may take place regardless of location, so that space-oriented protection is unable to avert the specific endangerment of the information technology system. Insofar as the infiltration uses the connection of the com- 194

puter concerned to form a computer network, it leaves spatial privacy provided by delimitation of the dwelling unaffected. The location of the system is in many cases of no interest for the investigation measure, and frequently will not be recognisable even for the authority. This applies in particular to mobile information technology systems such as laptops, Personal Digital Assistants (PDAs) or mobile telephones.

Article 13.1 of the Basic Law also does not provide protection against the collection, facilitated by infiltration of the system, of data found in the working memory or on the storage media of an information technology system located in a dwelling (see on the parallel relationship of home searches and seizure BVerfGE 113, 29 (45)). 195

cc) The manifestations of the general right of personality, in particular the guarantees of the protection of privacy, and of the right to informational self-determination, previously recognised in the case-law of the Federal Constitutional Court, also do not comply sufficiently with the special need for protection of the user of information technology systems. 196

(1) In its manifestation as protection of privacy, the general right of personality of the individual guarantees a spatially and thematically specified area which is to remain, in principle, free of undesired inspection (see BVerfGE 27, 344 (350 et seq.); 44, 353 (372-373); 90, 255 (260); 101, 361 (382-383)). The need for protection of the user of an information technology system is however not solely restricted to data to be allotted to his or her privacy. Such an attribution also frequently depends on the context in which the data came about and into which it is brought by linking with other data. In many cases, the data itself does not reveal what significance it has for the person concerned and which it may gain by inclusion in other contexts. The consequence of this is that, inevitably, not only private data is collected by the infiltration of the system, but access to all data is facilitated, so that a comprehensive picture of the user of the system may emerge. 197

(2) The right to informational self-determination goes beyond the protection of privacy. It confers on the individual, in principle, the power to determine for himself or herself the disclosure and use of his or her personal data (see BVerfGE 65, 1 (43); 84, 192 (194)). It supports and expands the protection of freedom of conduct and privacy in terms of fundamental rights by already making it start at the level of endangerment of the personality. Such an endangerment situation can already arise in the run-up to concrete threats to specific legal interests, in particular if personal information can be used and linked in a manner which the person concerned can neither detect nor prevent. The extent of protection of the right to informational self-determination is not restricted here to information which is already sensitive by its nature and hence already protected by fundamental rights. Depending on the purpose of access and the existing processing and linking facilities, the use of personal data which per se has only little information content can also have an impact on the privacy and freedom of conduct of the person concerned in terms of fundamental rights (see Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristis-* 198

che Wochenschrift 2007, p. 2464 (2466)).

199 The endangerments of personality to be averted with the right to informational self-determination emerge from the manifold possibilities open to the state, and where appropriate also to private players (see Federal Constitutional Court, Order of the 1st Chamber of the First Senate of 23 October 2006 – 1 BvR 2027/02 –, *Juristenzeitung* 2007, p. 576) to collect, process and use personal data. Such information may lead to the creation of further information, above all using electronic data processing, and to conclusions which may both impair the interests of the person concerned in confidentiality, which are protected by fundamental rights, and entail encroachments on his or her freedom of conduct (see BVerfGE 65, 1 (42); 113, 29 (45-46); 115, 320 (342); Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2466)).

200 However, the right to informational self-determination does not fully consider elements of personality endangerments which emerge from the fact that the individual relies on the use of information technology systems for his or her personality development, and in such instances entrusts personal data to the system or inevitably provides such data already by using the system. A third party accessing such a system can obtain data stocks which are potentially extremely large and revealing without having to rely on further data collection and data processing measures. In its severity for the personality of the person concerned, such access goes beyond individual data collections against which the right to informational self-determination provides protection.

201 d) Insofar as no adequate protection exists against endangerments of the personality emerging from the individual relying on the use of information technology systems for his or her personality development, the general right of personality accounts for the need for protection in its loophole-filling function over and above its manifestations recognised thus far by virtue of the fact that it guarantees the integrity and confidentiality of information technology systems. In the same way as the right to informational self-determination, this right is based on Article 2.1 in conjunction with Article 1.1 of the Basic Law; it protects the personal and private life of the subjects of the fundamental rights against access by the state in the area of information technology also insofar as the state has access to the information technology system as a whole, and not only to individual communication events or stored data.

202 aa) However, not all information technology systems which are able to create, process or store personal data require the special protection of a separate guarantee of personality rights. Insofar as such a system by its technical construction only contains data with a partial connection to a certain area of life of the person concerned – for instance non-networked electronic control systems in household appliances –, state access to the existing data is no different in qualitative terms than other data collections. In such a case, the protection of the right to informational self-determination is sufficient to guarantee the justified interests of the person concerned in confiden-

tiality.

The fundamental right to the guarantee of the integrity and confidentiality of information technology systems is to be applied, by contrast, if the empowerment to encroach covers systems which alone or in their technical networking can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of the personality. Such a possibility applies for instance to access to personal computers, regardless of whether they are installed in a fixed location or are operated while on the move. It is possible as a rule to conclude not only as regards use for private purposes, but also with business use, possible characteristics or preferences from the usage pattern. Specific fundamental right-related protection also covers for instance mobile telephones or electronic assistants which have a large number of functions and can collect and store many kinds of personal data. 203

bb) What is first of all protected by the fundamental right to the guarantee of the confidentiality and integrity of information technology systems is the interest of the user in ensuring that the data which are created, processed and stored by the information technology system that is covered by its scope of protection remain confidential. An encroachment on this fundamental right is also to be presumed to have taken place if the integrity of the protected information technology system is affected by the system being accessed such that its performance, functions and storage contents can be used by third parties; the crucial technical hurdle for spying, surveillance or manipulation of the system has then been overcome. 204

(1) The general right of personality in the manifestation dealt with here in particular provides protection against secret access, by means of which the data available on the system can be spied on in its entirety or in major parts. The fundamental right-related protection covers both the data stored in the working memory and also that which is temporarily or permanently kept on the storage media of the system. The fundamental right also protects against data collection using means which are technically independent of the data processing events of the information technology system in question, but the subject-matter of which is these data processing events. This is for instance the case with use of so-called hardware keyloggers or in measuring the electromagnetic radiation from monitors or keyboards. 205

(2) The fundamental right-related protection of the expectation of confidentiality and integrity exists regardless of whether access to the information technology system can be achieved easily or only with considerable effort. An expectation of confidentiality and integrity to be recognised from the fundamental rights perspective however only exists insofar as the person concerned uses the information technology system as his or her own, and hence may presume according to the circumstances that he or she alone or together with others entitled to use it disposes of the information technology system in a self-determined manner. Insofar as the use of the personal informa- 206

tion technology system takes place via information technology systems which are at the disposal of others, the protection of the user also covers this.

2. The fundamental right to the guarantee of the confidentiality and integrity of information technology systems is not unrestricted. Encroachments may be justified both for preventive purposes, and for criminal prosecution. The individual must only accept such restrictions of his or her right which are based on a statutory foundation that is constitutional. This is missing in the empowerment of the constitution protection authority to carry out preventive measures to be reviewed in the instant case. 207

a) The impugned provision does not meet the principle of the clarity of provisions and determinedness of provisions. 208

aa) The principle of determinedness finds its basis in the principle of the rule of law (Article 20 and Article 28.1 of the Basic Law) also with regard to the general right of personality in its various manifestations (see BVerfGE 110, 33 (53, 57, 70); 112, 284 (301); 113, 348 (375); 115, 320 (365)). It is to ensure that the democratically legitimised parliamentary legislature itself takes the essential decisions on encroachments on fundamental rights and the extent of the encroachments, that the Government and the administration find steering and restricting action standards in the statute, and that the courts can carry out judicial review. Furthermore, the clarity and determinedness of the provision ensure that the person concerned can realise the legal situation and can adjust to possible burdensome measures (see BVerfGE 110, 33 (52 et seq.); 113, 348 (375 et seq.)). The parliamentary legislature must determine the occasion, purpose and limits of the encroachment in a manner that is sufficiently area-specific, precise and clear in terms of its wording (see BVerfGE 100, 313 (359-360, 372); 110, 33 (53); 113, 348 (375); Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2466)). 209

Depending on the task to be accomplished, the legislature finds a variety of possibilities to provide the preconditions for the encroachment. The requirements of the principle of determinedness also depend on these regulatory possibilities (see BVerfGE 110, 33 (55-56); Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2467)). If the legislature uses indefinite legal concepts, the remaining uncertainties may not go so far that the predictability and justiciability of the action of the state agencies empowered by the provisions are endangered (see BVerfGE 21, 73 (79-80); 31, 255 (264); 83, 130 (145); 102, 254 (337); 110, 33 (56-57); Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2467)). 210

bb) According to these standards, § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act does not satisfy the principle of the clarity of provisions and determinedness of provisions insofar as the factual preconditions of the regulated measures cannot be sufficiently derived from the statute. 211

(1) The preconditions for measures according to § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act can be determined via two legislative referrals. Firstly, § 5.2 of the North Rhine-Westphalia Constitution Protection Act refers in general terms to § 7.1 of the North Rhine-Westphalia Constitution Protection Act, which in turn refers to § 3.1 of the North Rhine-Westphalia Constitution Protection Act. Accordingly, the deployment of intelligence service means is permissible if information relevant to the protection of the constitution can be obtained by these means. Secondly, § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act refers to the more stringent preconditions of the Act re Article 10 of the Basic Law for a case in which a measure according to § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act encroaches on the secrecy of correspondence, post and telecommunication or is equivalent to such encroachment in terms of its nature and grievousness. 212

(2) It is not compatible with the principle of the clarity of provisions and determinedness of provisions that § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act makes the reference to the Act re Article 10 of the Basic Law contingent on whether a measure encroaches on Article 10 of the Basic Law. The answer to the question of which fundamental rights are encroached on by investigation measures taken by the constitution protection authority can require complex assessments and evaluations. They are first and foremost incumbent on the legislature. It cannot avoid its task of giving concrete form to the relevant fundamental rights by means of corresponding statutory precautions by passing on the decision on how this fundamental right is to be concretised and implemented to a statute-executing administration through a mere factual reference to a possibly relevant fundamental right. Such “escape clause” legislative technique does not comply with the principle of determinedness in a provision such as § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act, which provides for new types of investigation measures which are intended to react to recent technological developments. 213

The breach of the principle of the clarity of provisions is made even more profound by the addition contained in § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act that the reference to the Act re Article 10 of the Basic Law also applies if an investigation measure is equivalent by its “nature and grievousness” to an encroachment on Article 10 of the Basic Law. Hence, the factual preconditions of regulated access are made contingent upon an evaluating comparison being carried out between this access and a measure which would have to be regarded as an encroachment on a specific fundamental right. § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act does not contain any standards for this comparison. If the factual preconditions cannot be adequately specified by merely referring to a specific fundamental right, this certainly applies to a provision which provides for such a comparison of the regulated measure on which there is no further statutory instruction with an encroachment on a specific fundamental right. 214

(3) The reference to the Act re Article 10 of the Basic Law in § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act also does not comply with the principle of the clarity of provisions and of the determinedness of provisions insofar as the range of the reference is not regulated with an adequate level of determinedness. 215

§ 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act refers to the “preconditions” of the Act re Article 10 of the Basic Law. The provision hence largely leaves unclear the parts of the Act re Article 10 of the Basic Law to which the reference is intended to be made. It does not reveal whether only the substantive encroachment threshold regulated in § 3 of the Act re Article 10 of the Basic Law is to be understood by the preconditions of this Act, or whether further provisions are also intended to be referred to. For instance, the procedural rules contained in §§ 9 et seq. of the Act re Article 10 of the Basic Law could also be included among the preconditions for an encroachment according to this statute. It would at least be conceivable to further refer to both the substantive encroachment thresholds and also to all procedural precautions of the Act re Article 10 of the Basic Law, as has been proposed by the Government of the *Land* North Rhine-Westphalia. Accordingly, the provisions on dealing with collected data contained in § 4 of the Act re Article 10 of the Basic Law and the provisions of §§ 14 et seq. of the Act re Article 10 of the Basic Law on parliamentary control would also be covered, although these provisions contain regulations which are not to be complied with until after an encroachment has taken place, and hence linguistically can hardly be counted among the preconditions for encroachment. 216

It is not evident that the undetermined version of the Act is due to particular legislative difficulties. The legislature could easily have listed in the referring provision those provisions of the Act re Article 10 of the Basic Law to which the reference was intended to be made. 217

b) § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act also does not comply with the principle of proportionality. The latter demands that an encroachment on fundamental rights should serve a legitimate purpose and be suitable, necessary and appropriate as a means to this end (see BVerfGE 109, 279 (335 et seq.); 115, 320 (345); Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2468); established case-law). 218

aa) The data collections provided for in the impugned provision serve the constitution protection authority in the performance of its tasks according to § 3.1 of the North Rhine-Westphalia Constitution Protection Act, and hence serve to secure, in the run-up to concrete dangers, the free democratic fundamental order, the continued existence of the Federation and of the *Länder*, as well as certain interests of the Federal Republic directed at international relations. Here, according to the reasoning of the Act, one of the goals pursued in particular with the revision of the Constitutional Pro- 219

tection Act was to ensure an effective fight against terrorism by the constitution protection authority in view of new risks, in particular connected with Internet communication (see *Landtag* document 14/2211, p. 1). However, the area of application of the revision is not restricted to the fight against terrorism, either explicitly or as a consequence of the systematic context. The provision requires a justification for its entire area of application.

The security of the state as a power securing peace and order which has a constitutional structure, and the security which it is to provide for the population against dangers to life, limb and freedom are constitutional values ranking equally with other high-value interests (see BVerfGE 49, 24 (56-57); 115, 320 (346)). The duty to protect has its foundation both in Article 2.2 sentence 1 and in Article 1.1 sentence 2 of the Basic Law (see BVerfGE 115, 118 (152)). The state complies with its constitutional mandate by countering dangers from terrorist or other activities. The increased use of electronic or digital means of communication and their penetration into almost all areas of life makes it more difficult for the constitution protection authority to perform its tasks effectively. Also, modern information technology offers extremist and terrorist groups many possibilities to establish and maintain contacts, as well as to plan and prepare, as well as to commit criminal offences. Legislative measures opening up information technology for state investigations in particular are to be seen against the background of the shift from traditional forms of communication to electronic message traffic and the possibilities to encrypt or conceal files (see on criminal prosecution BVerfGE 115, 166 (193)). 220

bb) Secret access to information technology systems is suitable to serve these purposes. It expands the possibilities available to the constitution protection authority for reconnaissance of threat situations. The legislature is granted considerable latitude in the evaluation of suitability (see BVerfGE 77, 84 (106); 90, 145 (173); 109, 279 (336)). It is not evident that this latitude has been exceeded here. 221

The power contained in § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act does not lose its suitability simply because, according to an evaluation put forward in legal literature (see for instance Buermeyer, *Höchstrichterliche Rechtsprechung im Strafrecht* 2007, p. 154 (165-166); Gercke, *Computer und Recht* 2007, p. 245 (253); Hornung, *Datenschutz und Datensicherheit* 2007, p. 575 (579)) and heard from the experts in the oral hearing, the person concerned has technical possibilities of protection in order at least to effectively prevent access in which the infiltration of the target system is carried out with the aid of access software. In the context of the suitability examination, it should not be required that measures which are permitted by the impugned provision always or even only as a rule promise success. The statutory prognosis that access of the regulated nature can be successful in an individual case is at least not evidently erroneous. It cannot be supposed to be taken for granted that each possible target person uses the possibilities for protection available against this and actually implements them free of error. Moreover, it appears to be conceivable that access possibilities will emerge in the 222

course of the further information technology development for the constitution protection authority which technically can no longer be prevented, or only with disproportionate effort.

Further, the suitability of the regulated empowerment is also not to be denied simply because the evidentiary value of the information obtained using access is possibly limited. It is submitted in this respect that technical authentication of the collected data is in principle conditional on exclusive control of the target system at the time in question (see Hansen/Pfitzmann, *Deutsche Richterzeitung* 2007, p. 225 (228)). However, these difficulties in securing evidence do not lead to a situation in which the collected data is devoid of value as information. What is more, according to the impugned provision, online access does not serve directly to obtain evidence for criminal proceedings which will stand up to an appeal on points of law, but is to provide the constitution protection authority with knowledge on the reliability of which less stringent requirements are to be placed due to the different nature of the task of the constitution protection authority as regards prevention in the run-up to concrete dangers than is the case in criminal proceedings. 223

cc) Secret access to information technology systems also does not violate the principle of necessity. In the context of its prerogative of assessment, the legislature may presume that no path which is equally effective, but less burdensome for the person concerned, exists to collect the data that is available on such systems. 224

In principle, an open search of the target system – not provided for in the Constitution Protection Act – is to be regarded as a less intrusive means in comparison with secret access (see Hornung, *Datenschutz und Datensicherheit* 2007, p. 575 (580)). If, however, the constitution protection authority has sufficient grounds to view the files stored on the storage media of an information technology system comprehensively in the performance of its tasks – including encrypted data –, to follow changes for a longer period or to comprehensively monitor the use of the system, it is not evident that there are less intrusive means to attain these investigation goals. The same applies to access to encrypted contents of Internet communication insofar as access to the transmission channel has no prospects of success. 225

dd) § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act however does not comply with the principle of appropriateness in the narrower sense. 226

This principle requires that the gravity of the encroachment, in an overall evaluation, may not be disproportionate to the gravity of the reasons justifying it (see BVerfGE 90, 145 (173); 109, 279 (349 et seq.); 113, 348 (382); established case-law). The legislature must appropriately attribute the individual interest encroached on by an encroachment on fundamental rights to the general interests served by the encroachment. A review carried out according to these standards can lead to a situation in which means may not be used to implement general interests because the impairments of fundamental rights emanating from it are more weighty than the interests to 227

be implemented (see BVerfGE 115, 320 (345-346); Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2469)).

§ 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act does not comply with this. The measures provided for in this norm entail encroachments on fundamental rights which are so intensive that they are disproportionate to the public investigation interest emerging from the regulated occasion for the encroachment. What is more, there is a need for supplementary procedural requirements in order to account for the interests of the person concerned protected by fundamental rights; these are also missing. 228

(1) § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act grants powers to perform encroachments of high intensity on fundamental rights. 229

(a) Data collection by the state from complex information technology systems shows considerable potential for researching the personality of the person concerned. This already applies to one-off, partial access, such as the seizure or copying of storage media of such systems (see re such case constellations for instance BVerfGE 113, 29; 115, 166; 117, 244). 230

(aa) Such secret access to an information technology system provides the acting state agency with access to a stock of data which may far exceed traditional sources of information in terms of its scope and diversity. This is a result of the many different possibilities for use offered by complex information technology systems which are associated with the creation, processing and storage of personal data. In particular, according to the current habits of use, such appliances are typically used deliberately to also store personal data of increased sensitivity, for example private text, pictorial or sound files. The available data stock may include detailed information on personal circumstances and on the life of the person concerned, the private and business correspondence made via various communication channels, or indeed diary-like personal records. 231

State access to such comprehensive data stocks entails the obvious risk that the collected data in an overall view facilitates comprehensive conclusions to be drawn on the personality of the person concerned, ranging to the formation of conduct and communication profiles. 232

(bb) Insofar as data is collected which provides information on the communication of the person concerned with third parties, the intensity of the encroachment on fundamental rights is further increased by virtue of the fact that the possibility for the citizen to participate in telecommunication without being monitored – also within the public good – is restricted (see on the collection of connection data BVerfGE 115, 166 (187 et seq.)). Collection of such data indirectly impairs the freedom of the citizen because he or she may be prevented from engaging in uninhibited individual communication 233

by fear of surveillance, even if surveillance does not take place until after the fact. What is more, such data collection shows in this respect a considerable spread, which increases the gravity of the encroachment, given that data collection of necessity covers communication partners of the target person, i.e. third parties, without it being necessary for the preconditions for such access to apply to these persons (see on telecommunication surveillance BVerfGE 113, 348 (382-383); furthermore BVerfGE 34, 238 (247); 107, 299 (321)).

(b) The gravity of the encroachment on fundamental rights is particularly severe if – as provided for by the impugned provision – secret technical infiltration facilitates the longer-term surveillance of the use of the system and the ongoing collection of the data in question. 234

(aa) The scope and diversity of the data stock which can be obtained by such access are still much larger than with one-off, partial data collection. Access also makes available to the investigation authority volatile data that is only kept in the working memory, or data only temporarily stored on the storage media of the target system. It also makes it possible to track the entire Internet communication of the person concerned over a longer period. Moreover, the spread of the investigative measure can be increased if the target system is included in a (local) network to which access is expanded. 235

Volatile data or data stored only temporarily can be particularly relevant to the personality of the person concerned, or can facilitate access to further, particularly sensitive data. This applies for instance to cache storage, which is established by service programs such as Web browsers, the evaluation of which can facilitate conclusions on the use of such programs, and hence indirectly on the preferences or communication habits of the person concerned, or for passwords, with which the person concerned gains access to technically secured contents on his or her system or the network. What is more, longer-term surveillance of Internet communication, as facilitated by the impugned provision in comparison to one-off collection of communication contents and communication circumstances, also constitutes a considerably more intensive encroachment. Finally, it should be considered that regulated access is intended and suitable amongst other things to circumvent the deployment of encryption technology. This overcomes the individual precautions taken by the person concerned to protect himself or herself against access to data not authorised by him or her. The prevention of such informational self-protection increases the gravity of the encroachment on fundamental rights. 236

Also the risk of the formation of conduct and communication profiles increases by virtue of the possibility of comprehensively monitoring the use of the target system for a longer period. By these means, the authority can largely research the personal circumstances and the communication conduct of the person concerned. Such comprehensive collection of personal data is to be regarded as a particularly intense encroachment on fundamental rights. 237

(bb) The encroachment intensity of regulated access is further determined by its secrecy. The secrecy of state encroachment measures is the exception in a state based on the rule of law, and it requires special justification (see Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2469-2470)). If the persons concerned learn of a state measure burdening them prior to its execution, they can defend their interests from the outset. They can, firstly, take legal steps to prevent it, for instance by seeking recourse to a court. Secondly, they have the possibility with open data collection to exert a de facto influence on the course taken by the investigation via their conduct. The exclusion of this opportunity to exert an influence increases the gravity of the encroachment on fundamental rights (see on legal possibilities of aversion BVerfGE 113, 348 (383-384); 115, 320 (353)). 238

(cc) The weight of the encroachment is characterised, finally, by dangers arising as a result of access for the integrity of the access computer and for legal interests of the person concerned, or also of third parties. 239

The experts heard in the oral hearing have stated that it could not be ruled out that access itself could even cause damage to the computer. For instance, interactions with the operating system could lead to data loss (see also Hansen/Pfitzmann, *Deutsche Richterzeitung* 2007, p. 225 (228)). It should also be considered that there is no mere reading access as a result of infiltration. Both the accessing agency and third parties which might misuse the access program can delete, alter or create new data stocks by accident or by deliberate manipulation because of the infiltration of the access computer. This may harm the person concerned in many ways which may or may not be connected to the investigations. 240

Depending on the infiltration technology deployed, infiltration may also cause further damage which must be considered in examining the appropriateness of a state measure. If the person concerned is for instance supplied with infiltration software in the shape of an allegedly useful program, it cannot be ruled out that he or she might pass on this program to third parties whose systems could also be damaged as a result. If previously unknown security loopholes in the operating system are used for infiltration, this might cause a conflict of goals between the public interest in successful access and in the greatest possible security of information technology systems. As a result, the danger exists that the investigation authority might for instance omit suggesting to other agencies measures to close such security loopholes, or might even actively endeavour to ensure that the loopholes remain undiscovered. The goal conflict might hence impair the trust of the population in state endeavours to ensure the greatest possible security of information technology. 241

(2) In view of its intensity, the encroachment on fundamental rights lying in secret access to an information technology system in the context of a preventive goal only satisfies the principle of appropriateness if certain facts indicate a danger posed to a predominantly important legal interest in the individual case, even if it cannot yet be 242

ascertained with sufficient probability that the danger will arise in the near future. What is more, the statute granting powers to perform such an encroachment must ensure the protection of the fundamental rights of the person concerned also by means of suitable procedural precautions.

(a) In the tension between the obligation incumbent on the state to protect legal interests and the interest of the individual in respect for his or her rights as guaranteed by the constitution, the task of the legislature includes in an abstract form achieving compensation between the conflicting interests (see BVerfGE 109, 279 (350)). This may lead to a situation in which certain intensive encroachments on fundamental rights may be provided only to protect certain legal interests, and only from certain suspicion or danger levels onwards. The obligations incumbent on the state to protect other legal interests also come up against their limits in the prohibition of inappropriate encroachments on fundamental rights (see BVerfGE 115, 320 (358)). Corresponding encroachment thresholds are to be guaranteed by a statutory provision (see BVerfGE 100, 313 (383-384); 109, 279 (350 et seq.); 115, 320 (346)). 243

(b) A highly intensive encroachment on fundamental rights can already be disproportionate as such if the statutorily regulated occasion for the encroachment does not show sufficient gravity. Insofar as the relevant statute serves to avert certain dangers, as is the case for the Constitution Protection Act under § 1 of the North Rhine-Westphalia Constitution Protection Act, it is the rank and the nature of the endangerment of protected interests referred to in the respective provision which is relevant to the gravity of the occasion for encroachment (see BVerfGE 115, 320 (360-361)). 244

If the protected interests as such standing behind an empowerment to encroach are sufficiently prevalent to justify encroachments on fundamental rights of the regulated type, the principle of proportionality gives rise to constitutional requirements being placed on the factual preconditions of the encroachment. In this respect, the legislature has to maintain a balance between the nature and intensity of the impairment of fundamental rights on the one hand and the factual elements constituting an entitlement to encroachment on the other hand (see BVerfGE 100, 313 (392 et seq.)). The requirements as to the degree of probability and the factual basis of the prognosis must be proportionate to the nature and gravity of the impairment of fundamental rights. Even with the greatest weight of the threatening legal interest in encroachment, it is not possible to forgo the requirement of sufficient probability of occurrence. It must also be guaranteed as a precondition for a grave encroachment on fundamental rights that presumptions and conclusions have a starting point in fact which has a concrete outline (see BVerfGE 113, 348 (386); 115, 320 (360-361)). 245

(c) The principle of proportionality restricts a statutory provision granting powers to effect secret access to information technology systems initially insofar as special requirements exist as to the occasion for the encroachment. The latter consists here of risk aversion in the context of the tasks of the constitution protection authority according to § 1 of the North Rhine-Westphalia Constitution Protection Act. 246

(aa) Such an encroachment may only be provided for if the empowerment to encroach makes it contingent on the existence of factual indications of a concrete danger to a predominantly important legal interest. Predominantly important are first of all life, limb and freedom of the individual. Further, predominantly important are such interests of the public a threat to which affects the basis or the continued existence of the state or the basis of human existence. This also includes for instance the functionality of major parts of existence-ensuring public supply facilities. 247

A state measure by means of which – as here – the personality of the person concerned is revealed to broad surveillance by the investigation authority is in principle not appropriate to protect other legal interests of individuals or of the public in situations not giving rise to an existential threat. For the protection of such legal interests, the state must restrict itself to other investigation powers granted to it by the respectively applicable non-constitutional law in the area of prevention. 248

(bb) The statutory basis of empowerment must furthermore provide as a precondition for secret access that at least factual indications exist of a concrete danger to the sufficiently weighty protected interests of the provision. 249

α) The requirement of factual indications leads to a situation in which presumptions or general experience are not sufficient to justify access by themselves. Rather, certain facts that substantiate a prognosis of danger must be ascertained (see BVerfGE 110, 33 (61); 113, 348 (378)). 250

This prognosis must relate to the development of a concrete danger. This is a factual situation in which the sufficient probability exists in an individual case that damage will be caused by specific persons to the interests protected by the provision in the foreseeable future without action being taken on the part of the state. The concrete danger is determined by three criteria: the individual case, the immanent risk that a danger will become actual damage, and the reference to individuals as triggers. Access to the information technology system to be assessed here can however already be justified if it cannot yet be ascertained with sufficient probability that the danger will arise in the near future, if certain facts indicate a danger posed to a predominantly important legal interest in the individual case. The facts must, firstly, permit a conclusion concerning events which at least by their nature are concrete and predictable in time, and secondly permit to conclude that specific individuals will be involved about whose identity it is at least known that the surveillance measures can be deployed against them in a targeted manner and largely restricted to them. 251

By contrast, the weight of the encroachment on fundamental rights which is constituted by secret access to an information technology system is not sufficiently accommodated if the actual occasion for the encroachment is shifted still further into the run-up to a concrete danger to the interests protected by the provision that is not yet predictable in detail. 252

It is constitutionally unacceptable to link the intervention threshold to the run-up 253

stage in view of the gravity of the encroachment if events are known only by relatively diffuse indications of possible dangers. The factual situation is then frequently marked by a high degree of ambivalence of the significance of individual observations. The events can remain in harmless contexts, but can also constitute the commencement of an event culminating in danger (see on the prevention of criminal offences BVerfGE 110, 33 (59)).

β) The constitutional requirements placed on the regulation of the actual occasion for the encroachment are to be respected in the case of secret access to an information technology system for all empowerments to effect an encroachment which have a preventive objective. Since the impairment caused by the encroachment is the same in all these cases for the persons concerned, there is no reason as to its requirements for authority-related distinction, such as between police authorities and other authorities entrusted with preventive tasks, such as constitution protection authorities. It is in principle without relevance for the weighting of secret access to an information technology system that police and constitution protection authorities have different tasks and powers, and in consequence can execute measures with differing levels of encroachment. 254

It is true at the same time that there are distinctions between the empowerments of the various authorities with preventive tasks which can be justified against the standard of the constitution. The special purposes in the field of strategic telecommunication surveillance by the Federal Intelligence Service (*Bundesnachrichtendienst*) do justify that the preconditions for encroachment are determined differently than in police law or in the law of criminal procedure (see BVerfGE 100, 313 (383)). The preconditions for intervention for investigative measures can also be differently structured, depending on which authority carries them out and what objective they have in mind. Thus, the special tasks of the constitution protection authorities can for instance be taken into account for reconnaissance of anti-constitutional activities in the run-up to concrete dangers (see in general terms on the problem of adequate investigation regulations during the run-up stage Möstl, *Deutsches Verwaltungsblatt – DVBl* 2007, p. 581; Volkmann, *Juristenzeitung* 2006, p. 918). It is hence in principle constitutionally unobjectionable that the constitution protection authorities may also deploy intelligence service means in order to obtain information about groups which act against the interests protected by the Constitution Protection Act – at least for the time being – by legal means. It is also not to be required for the deployment of such means in general terms that concrete suspicion should exist over and above the factual indications that are always required for such activities (see for instance § 7.1 no. 1 in conjunction with § 3.1 of the North Rhine-Westphalia Constitution Protection Act). 255

However, the legislature is also bound by constitutional requirements emerging from the principle of proportionality with the regulation of the individual powers of security authorities whose task consists of preliminary reconnaissance. This may mean that also those authorities may only be empowered to carry out certain intensive encroachments on fundamental rights if more stringent requirements are met as to the 256

regulation of the occasion for the encroachment. This applies for instance particularly to secret access to an information technology system which entails a risk that the person concerned is rendered vulnerable to a broad state investigation of his or her personality, regardless of the authority carrying it out. Even if it were not to be possible to develop statutory measures which are specifically tailored to authorities which act in the run-up stage to the occasion for the encroachment which comparably account for the gravity and the intensity of the endangerment of fundamental rights in a manner comparable to that which is for instance provided by the traditional definition of danger in police law, this would not be a constitutionally acceptable occasion to reduce the factual preconditions for an encroachment of the nature at hand.

(d) Furthermore, empowerment to effect secret access to information technology systems must be linked with suitable statutory precautions in order to secure the interests of the person concerned under procedural law. If a norm provides for secret investigation activities on the part of the state which – as here – affect particularly protected zones of privacy or demonstrate a particularly high intensity of encroachment, the weight of the encroachment on fundamental rights is to be accounted for by suitable procedural precautions (see Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2471), with further references). In particular, access is in principle to be placed under the reservation of a judicial order. 257

(aa) Such reservation facilitates the preventive control of a planned secret investigation measure by an independent and neutral control body. Such control may constitute a significant element of the effective fundamental rights protection. It is not suited to compensate for the shortcomings of an encroachment threshold which is regulated too undeterminedly, or one which is set too low, since the independent review instance can only ensure that the regulated preconditions for encroachment are respected (see BVerfGE 110, 33 (67-68)). It can however guarantee that the decision on a secret investigation measure takes sufficient account of the interests of the person concerned if the person concerned himself or herself is unable to take measures in advance to defend his or her interests because of the secret nature of the measure. In this respect, the control serves the purpose of the “compensatory representation” of the interests of the person concerned in the administrative procedure (see Saxon Constitutional Court (*SächsVerfGH*), Judgment of 14 May 1996 – Vf.44-II-94 –, *Juristenzeitung* 1996, p. 957 (964)). 258

(bb) If a secret investigation measure leads to a grievous encroachment on fundamental rights, preventive control by an independent body is constitutionally required because the person concerned would otherwise remain unprotected. The legislature is however in principle granted latitude in legislating on the detailed structure of the control, such as in the decision on the controlling body and the applicable proceedings. In case of a particularly grievous encroachment on fundamental rights, such as secret access to an information technology system, the latitude is reduced such that the measure is in principle to be placed under the reservation of a judicial order. Be- 259

cause of their personal and factual independence, and because they are exclusively bound by the law, judges can best and most safely defend the rights of the person concerned in an individual case (see BVerfGE 103, 142 (151); 107, 299 (325)). This is however conditional on their carrying out a detailed examination of the lawfulness of the envisioned measure and on their recording the reasoning in writing (re the requirements as to ordering acoustic monitoring of dwellings see BVerfGE 109, 279 (358 et seq.); for criticism of the practice of the implementation of the requirement of a judicial order in house searches see BVerfGE 103, 142 (152), with further references).

The legislature may only entrust another body with control if this offers the same guarantee of its independence and neutrality as a judge. Such body must also submit reasoning as to lawfulness. 260

An exception may be provided from the requirement of previous control of the measure by a neutral body suited thereto in urgent cases, for instance in case of imminent danger, if it is ensured that a subsequent review will be carried out by the neutral body. There are in turn constitutional requirements for the factual and legal preconditions of the assumption of an urgent case (see BVerfGE 103, 142 (153 et seq.) re Article 13.2 of the Basic Law). 261

(3) According to these standards, the impugned provision does not meet the constitutional requirements. 262

(a) According to § 5.2 in conjunction with § 7.1 no. 1 and § 3.1 of the North Rhine-Westphalia Constitution Protection Act, preconditions for the deployment of intelligence service means by the constitution protection authority are only factual indications of the presumption that information on anti-constitutional activities can be obtained by these means. This is not a sufficient substantive encroachment threshold, either as to the factual preconditions for the encroachment, or to the weight of legal interests to be protected. Also, there is no provision for a prior examination by an independent body, so that the constitutionally required procedural security is lacking. 263

(b) These shortcomings do not cease to apply if the reference contained in § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act to the detailed preconditions according to the Act re Article 10 of the Basic Law, is included in the examination despite its undeterminedness, and, in the broad interpretation of the Government of the *Land* North Rhine-Westphalia, is understood to refer to all formal and substantive precautions of this Act. § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act does not restrict secret access to an information technology system to telecommunication surveillance, the preconditions for which are regulated by § 3.1 of the Act re Article 10 of the Basic Law, but facilitates such access in principle to obtain all available data. 264

Neither the regulation of the encroachment threshold, nor the procedural requirements of the encroachment elements provided for in § 3.1 of the Act re Article 10 of 265

the Basic Law, meet the constitutional requirements.

(aa) According to § 3.1 sentence 1 of the Act re Article 10 of the Basic Law, a surveillance measure is permissible if factual indications exist of the suspicion that someone is planning, is committing or has committed a criminal offence from a list that is regulated in the provision. The list of criminal offences, firstly, does not permit a concept to be recognised according to which it could be justified to take all the criminal offences listed there as an occasion for measures according to § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act. Hence, it is not ensured with all the provisions referred to that access in the concrete case serves to protect one of the predominantly important legal interests listed above (C I 2 b, dd (2) (c) (aa)). Secondly, the reference to § 3.1 sentence 1 of the Act re Article 10 of the Basic Law does not ensure in each case that secret access to an information technology system takes place only if such legal interests are endangered in an individual case with sufficient probability (C I 2 b, dd (2) (c) (bb)) in the near future. 266

According to § 3.1 sentence 2 of the Act re Article 10 of the Basic Law, a surveillance measure may also be ordered if factual indications exist of the suspicion that someone is a member of an association the purposes or activities of which are intended to commit criminal offences which are against the interests protected by the constitution. The criminal offences are however only described in general terms, so that the risk of an expanding interpretation exists which would also make possible an encroachment to protect legal interests which are not predominantly important. What is more, according to this provision, sufficient factual indications would not have to exist in each case in which the encroachment element of § 3.1 sentence 2 of the Act re Article 10 of the Basic Law is complied with, for a danger posed to a predominantly important legal interest by this person or association in the individual case. 267

(bb) § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act does not meet the constitutional requirements for preventive control of secret access to an information technology system, even if the reference to the Act re Article 10 of the Basic Law is included. 268

§ 10 of the Act re Article 10 of the Basic Law provides for prior ordering of the surveillance measure which is granted by the competent supreme *Land* authority in response to a request by the constitution protection authority. This procedure is not sufficient to ensure the preventive control required by Article 2.1 in conjunction with Article 1.1 of the Basic Law. The statute regulates neither the requirement of a judicial order, nor – since the provision of preventive control by the G 10 Commission contained in § 3.6 of the Act on the Implementation of the Act re Article 10 of the Basic Law is not included in the reference – an equivalent control mechanism. Unlike a court, the competent supreme *Land* authority may because of its departmental structure have its own interest in the execution of intelligence service measures of constitution protection. It does not offer the same guarantee of the independence and neutrality of control as a court. 269

c) Finally, there are no adequate statutory precautions to avoid encroachments on the absolutely protected core area of private life by measures according to § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act. 270

aa) Secret surveillance measures carried out by state agencies must respect an inviolable core area of private life the protection of which emerges from Article 1.1 of the Basic Law (see BVerfGE 6, 32 (41); 27, 1 (6); 32, 373 (378-379); 34, 238 (245); 80, 367 (373); 109, 279 (313); 113, 348 (390)). Even overriding interests of the public cannot justify encroachment on it (see BVerfGE 34, 238 (245); 109, 279 (313)). The development of the personality in the core area of private life includes the possibility to express inner events such as perceptions and feelings, as well as considerations, views and experiences of a highly personal nature, without fear that state agencies may have access to them (see BVerfGE 109, 279 (314)). 271

In the context of secret access to an information technology system, the danger exists that the state agency might collect personal data which is to be attributed to the core area. For instance, the person concerned may use the system to establish and store files with highly personal contents, such as diary-like records or private film or sound documents. Such files can enjoy absolute protection, as can for instance written embodiments of highly personal experiences (on this see BVerfGE 80, 367 (373 et seq.); 109, 279 (319)). Secondly, insofar as it is used for telecommunication purposes, the system can be used to transmit contents which can equally fall within the core area. This applies not only to speech telephony, but for instance also to telecommunication using e-mails or other Internet communication services (see BVerfGE 113, 348 (390)). The absolutely protected data can be collected with different types of access, such as with the inspection of storage media, just as with the surveillance of ongoing Internet communication or indeed with full surveillance of the use of the target system. 272

bb) In the event of secret access to the information technology system of the person concerned, there is a need for special statutory precautions protecting the core area of private life. 273

To manage their personal matters, and for use in telecommunication also with close persons, citizens increasingly use complex information technology systems which offer them development possibilities in the highly personal sphere. In view of this, an investigation measure such as access to an information technology system, using which the data available on the target system can be comprehensively collected, entails in comparison to other surveillance measures – such as the use of the Global Positioning System as a tool of technical monitoring (see on this BVerfGE 112, 304 (318)) – an increased danger of data being collected which have highly personal contents. 274

Because of the secrecy of access, the person concerned has no opportunity himself or herself to endeavour to ensure prior to or during the investigative measure that the 275

investigating state agency respects the core area of his or her private life. This complete loss of control is to be countered by special provisions which provide protection against the danger of a violation of the core area through suitable procedural precautions.

cc) The constitutional requirements as to the concrete structure of the protection of the core area can differ depending on the nature of the collection of the information and the information collected by it. 276

A statutory empowerment to carry out a surveillance measure which may affect the core area of private life must ensure as far as possible that no data is collected which relates to the core area. If – as with secret access to an information technology system – it is practically unavoidable to obtain information before its reference to the core area can be evaluated, sufficient protection must be ensured in the evaluation phase. In particular, data that is found and collected which refers to the core area must be deleted without delay and its exploitation must be ruled out (see BVerfGE 109, 279 (318); 113, 348 (391-392)). 277

(1) In the context of secret access to an information technology system, data collection will already be automated for technical reasons, at least in the vast majority of cases. The automation however makes it more difficult in comparison with monitoring carried out by individuals to make suitable distinctions when collecting data with and without reference to the core area. According to the view unanimously held by the experts heard by the Senate, technical search or exclusion mechanisms to determine relevance to the core area of personal data do not work so reliably that effective protection of the core area could be achieved with their aid. 278

Even if data access takes place directly by persons without first being recorded by technical means, for instance in the case of personal surveillance of speech telephony carried out via the Internet, protection of the core area already encounters practical difficulties when it comes to data collection. It is as a rule not predictable with certainty when such a measure is carried out what the contents of the collected data will be (see on telecommunication surveillance BVerfGE 113, 348 (392)). There may also be difficulties in analysing the contents of the data during collection. This applies for instance to foreign-language text documents or conversations. Also in such cases, the core area relevance of the monitored events cannot always be evaluated prior to or during data collection. In such cases, it is constitutionally not required to forgo access from the outset because of the risk of a breach of the core area at collection level, since access to the information technology system is based on factual indications of a concrete danger to a predominantly important protected interest. 279

(2) The constitutionally required protection of the core area can be guaranteed in the context of a two-tier protection concept. 280

(a) The statutory provision must endeavour to ensure that collection of data that is relevant to the core area is avoided as far as possible in terms of information technol- 281

ogy and investigation technique (see on telecommunication surveillance BVerfGE 113, 348 (391-392); on acoustic monitoring of dwellings BVerfGE 109, 279 (318, 324)). In particular, available information technology security devices are to be deployed. If there are concrete indications in an individual case that a certain data collection will affect the core area of private life, it must be avoided in principle. The situation is different if for instance concrete indications exist that core area-related communication contents are linked with contents which fall within the goal of the investigation in order to prevent surveillance.

(b) In many cases, the core area relevance of the collected data will not be ascertained prior to or during data collection. The legislature has to ensure by means of suitable procedural provisions that if data has been collected which relates to the core area of private life, the intensity of the violation of the core area and its impact on the personality and development of the person concerned remain as low as possible. 282

Decisive significance in terms of protection attaches to the viewing of the collected data as to contents which are relevant to the core area, for which suitable procedures are to be provided which sufficiently accommodate the interests of the person concerned. If viewing reveals that data was collected with relevance to the core area, it is to be deleted without delay. Passing on or exploitation is to be ruled out (see BVerfGE 109, 279 (324); 113, 348 (392)). 283

dd) The Constitution Protection Act does not contain the required provisions protecting the core area. Nothing else emerges if the reference in § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act to the Act re Article 10 of the Basic Law is included despite its undeterminedness. This statute also does not contain precautions to protect the core area of private life. 284

In contradistinction to the view taken by the Government of the *Land* North Rhine-Westphalia, § 4.1 of the Act re Article 10 of the Basic Law may not even be referred to if the reference of § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act is understood broadly such that it covers this provision. § 4.1 of the Act re Article 10 of the Basic Law only regulates that collected data is to be deleted which are not or are no longer needed, and hence regulates the general principle of necessity. The provision by contrast does not contain any special standards for the collection, viewing and deletion of data which can show a connection to the core area. The principle of necessity cannot be equated with constitutionally required respect for the core area of private life. The core area is rather in particular not amenable to being qualified by contrary investigation interests, as was explicitly introduced by the application of the principle of necessity (see BVerfGE 109, 279 (314)). 285

d) The violation of the general right of personality in its manifestation as providing protection of the confidentiality and integrity of information technology systems (Article 2.1 in conjunction with Article 1.1 of the Basic Law) leads to the nullity of § 5.2 no. 11 sentence 1 alternative 2 of the North Rhine-Westphalia Constitution Protection Act. 286

e) In view of this, there is no longer any need to review the degree to which measures permitted by the provision also violate other fundamental rights or the principle of specifying [the fundamental right which is restricted] contained in Article 19.1 sentence 2 of the Basic Law. 287

II.

The empowerment to secret reconnaissance of the Internet contained in § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act violates the secrecy of telecommunication guaranteed by Article 10.1 of the Basic Law. Measures according to this provision can in certain cases constitute an encroachment on this fundamental right which is constitutionally not justified (1); Article 19.1 sentence 2 of the Basic Law is also violated (2). Its unconstitutionality makes the provision null and void (3). The constitution protection authority may however continue to carry out measures of Internet reconnaissance insofar as these are not to be regarded as encroachments on fundamental rights (4). 288

1. The secret reconnaissance of the Internet regulated in § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act covers measures by means of which the constitution protection authority obtains knowledge of the contents of Internet communication via the channel technically provided therefor, in other words for instance by calling up a Web site on the World Wide Web using a Web browser (see above A I 1 a). In certain cases, this can encroach on the secrecy of telecommunication. Such an encroachment is constitutionally not justified by the impugned provision. 289

a) The area protected by Article 10.1 of the Basic Law covers the ongoing telecommunication carried out using an information technology system that is connected to the Internet (see above I 1 c, aa (1)). However, this fundamental right only protects the confidence of the individual that knowledge of the telecommunication in which he or she is involved is not being obtained by third parties. By contrast, the confidence of the communication partners in one another is not the subject-matter of the fundamental rights protection. If a state investigation measure does not focus on unauthorised access to telecommunication, but on the disappointment of the personal trust in the communication partner, this does not constitute an encroachment on Article 10.1 of the Basic Law (see BVerfGE 106, 28 (37-38)). The state's obtaining knowledge of the contents of telecommunication is hence only to be measured against the secrecy of telecommunication if a state agency monitors a telecommunication relationship from outside without itself being an addressee of the communication. By contrast, the fundamental right does not provide protection against a state agency itself establishing a telecommunication relationship with a subject of fundamental rights. 290

If a state agency obtains knowledge of the contents of telecommunication conducted via the communication services of the Internet via the channel technically provided therefor, this shall only constitute an encroachment on Article 10.1 of the Basic Law if 291

the state agency is not authorised to do so by those involved in the communication. Since the secrecy of telecommunication does not protect the mutual personal trust of those involved in communication, the state agency is already authorised to collect the communication contents if only one of several participants has permitted it such access voluntarily.

The secret reconnaissance of the Internet accordingly encroaches on Article 10.1 of the Basic Law if the constitution protection authority monitors secured communication contents by using access keys which it collected without authorisation or against the will of those involved in the communications. This is the case for instance if a password collected using keylogging is used in order to gain access to an e-mail inbox or to a closed chatroom. 292

By contrast, an encroachment on Article 10.1 of the Basic Law is to be denied if for instance a participant of a closed chatroom has voluntarily provided the person acting for the constitution protection authority with his or her access, and as a consequence the authority uses this access. Encroachment on the secrecy of telecommunication certainly does not apply if the authority collects generally accessible contents, for instance by viewing open discussion fora or Web sites which are not password protected. 293

b) The encroachments on Article 10.1 of the Basic Law facilitated by § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act are constitutionally not justified. The impugned provision does not meet the constitutional requirements as to empowerments to effect such encroachments. 294

aa) § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act does not comply with the principle of the clarity of provisions and determinedness of provisions since the preconditions for encroachment are not sufficiently precisely regulated because of the undeterminedness of subsection 2 of this provision (see above C I 2 a, bb). 295

bb) The impugned provision is furthermore not in compliance with the principle of appropriateness in the narrower sense insofar as it is to be measured against Article 10.1 of the Basic Law. 296

The encroachment on the secrecy of telecommunication is grievous. On the basis of the impugned provision, the constitution protection authority may access communication contents which may be sensitive in nature, and which may provide insight into the personal matters and habits of the person concerned. It is not only the one who gave rise to the surveillance measure who is concerned. The encroachment can rather show a certain spread if information is obtained not only on the communication conduct of the party against whom the measure is addressed, but also on his or her communication partners. The secrecy of access increases the intensity of the encroachment. Additionally, because of the broad wording of the preconditions for encroachment contained in § 7.1 no. 1 in conjunction with § 3.1 of the North Rhine- 297

Westphalia Constitution Protection Act, persons may also be monitored who have not given rise to the occasion for the encroachment.

Such a grievous encroachment on fundamental rights, even if the weight of the goals of protection of the constitution is taken into account, is in principle at least, also conditional on the provision of a qualified substantive encroachment threshold (see re criminal law investigations BVerfGE 107, 299 (321)). This is not the case here. Rather, § 7.1 no. 1 in conjunction with § 3.1 of the North Rhine-Westphalia Constitution Protection Act permits intelligence service measures to a considerable degree in the run-up to concrete endangerment without regard to the grievousness of the potential violation of legal interests, and also towards third parties. Such a broad empowerment to effect an encroachment is not compatible with the principle of proportionality. 298

cc) The Constitution Protection Act does not contain any precautions to protect the core area of private life in connection with encroachments according to § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act. Such provisions are however required insofar as a state agency is empowered to collect the contents of telecommunication by encroaching on Article 10.1 of the Basic Law (see BVerfGE 113, 348 (390 et seq.)). 299

2. Finally, § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act, insofar as the provision grants powers to effect encroachments on Article 10.1 of the Basic Law, does not comply with the principle of specifying the fundamental right restricted contained in Article 19.1 sentence 2 of the Basic Law. 300

According to Article 19.1 sentence 2 of the Basic Law, a statute must specify the fundamental right which is restricted by this statute or this Act, stating the relevant Article. The function of the principle of specifying the fundamental right restricted is to provide a warning and an occasion for reflection (see BVerfGE 64, 72 (79-80)). Specifying the encroachment contained in the wording of the Act is intended to ensure that the legislature only provides for encroachments of which it is aware as such, and with regard to which it accounts to itself as to their impact on the fundamental rights concerned (see BVerfGE 5, 13 (16); 85, 386 (404)). The fact of explicit specifying also makes it easier to clarify the necessity and the extent of the intended encroachment on fundamental rights in the public debate. By contrast, it is not sufficient for the legislature to have been aware of the encroachment on fundamental rights if this has not been reflected in the text of the Act (see BVerfGE 113, 348 (366-367)). 301

The impugned provision does not comply with the principle of specifying the fundamental right restricted with regard to Article 10.1 of the Basic Law. In contradistinction to the view taken by the Government of the *Land* North Rhine-Westphalia, the impugned provision does not meet the requirements simply because § 5.2 no. 11 sentence 2 of the North Rhine-Westphalia Constitution Protection Act may indicate by referring to the Act re Article 10 of the Basic Law that the legislature has considered an 302

encroachment on the secrecy of telecommunication to be possible. The principle of specifying the fundamental right restricted is only accounted for if the fundamental right is explicitly named in the text of the Act as being restricted. Moreover, in view of the fact that § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act contains two different empowerments to encroach, it by no means emerges from the statute with sufficient clarity for which of them the legislature at least anticipated the possibility of an encroachment on Article 10 of the Basic Law.

3. The violation of § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act against Article 10.1 and Article 19.1 sentence 2 of the Basic Law leads to the nullity of the provision. 303

4. The nullity of the empowerment however does not lead to a situation in which measures of Internet reconnaissance are in principle denied to the authority, insofar as these do not encroach on fundamental rights. 304

Insofar as it does not fall under Article 10.1 of the Basic Law, the secret reconnaissance of the Internet in particular does not always encroach on the general right of personality guaranteed by Article 2.1 in conjunction with Article 1.1 of the Basic Law. 305

a) The confidentiality and integrity of information technology systems guaranteed by the general right of personality is not affected by measures of Internet reconnaissance since measures according to § 5.2 no. 11 sentence 1 alternative 1 of the North Rhine-Westphalia Constitution Protection Act are restricted to data which the owner of the system has provided for Internet communication – for instance the operator of a Web server – using the channel technically provided therefor. The person concerned himself or herself has opened his or her system by technical terms for such data collections. He or she cannot rely on these not being carried out. 306

b) At least as a rule, an encroachment on Article 2.1 in conjunction with Article 1.1 of the Basic Law is also to be denied in its manifestation as a right to informational self-determination. 307

aa) The state is not in principle denied the possibility to obtain publicly accessible information. This also applies if personal information can be collected by these means in an individual case (see for instance Böckenförde, *Die Ermittlung im Netz*, 2003, p. 196- 197; Zöller, *Goltdammer's Archiv für Strafrecht* 2000, p. 563 (569)). There is hence no encroachment on the general right of personality if a state agency collects communication contents that are available on the Internet addressing all readers or at least a group of individuals that is not further delimitated. This is the case, for instance, if the authority calls up a generally accessible Web site on the World Wide Web, subscribes to a mailing list that is open to all comers or monitors an open chatroom. 308

An encroachment on the right to informational self-determination can however apply if information obtained by viewing generally accessible contents is deliberately compiled, stored and where appropriate evaluated using further data, and a special dan- 309

ger emerges from this for the personality of the person concerned. A basis for empowerment is required for this.

bb) An encroachment on the right to informational self-determination does not apply if a state agency enters a communication relationship with a subject of fundamental rights under a cover, but does apply if in doing so it exploits a trust that is worthy of protection of the person concerned in the identity and the motivation of a communication partner in order to gather personal data which it would otherwise not receive (see re investigations by undercover investigators Federal Administrative Court – BVerwG, Judgment of 29 April 1997 – 1 C 2/95 –, *Neue Juristische Wochenschrift* 1997, p. 2534; Di Fabio, in: Maunz/Dürig, *GG*, *Art. 2.1*, marginal no. 176; Duttge, *Juristenzeitung* 1996, p. 556 (562-563); Murswiek, in: Sachs, *GG*, 4th ed., 2007, Article 2 marginal no. 88 b; Warntjen, *Geheime Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung*, 2007, p. 163; specifically re investigations on the Web Germann, *Gefahrenabwehr und Strafverfolgung im Internet*, 2000, pp. 519 et seq.). 310

Accordingly, pure Internet reconnaissance will not as a rule bring about an encroachment on fundamental rights. The communication services of the Internet facilitate to a large degree the expansion of communication relationships in the context of which the trust of a communication partner in the identity and truthfulness of his or her communication partners is not worthy of protection since no examination mechanisms are available for it. This also applies if certain persons – for instance in the context of a discussion forum – participate in the communication over a longer period and by these means a kind of “electronic community” has formed. Also in the context of such a communication relationship, each participant is aware that he or she does not know the identity of his or her partner, or at least is unable to examine his or her information about himself or herself. His or her trust that he or she is not communicating with a state agency is, as a consequence, not worthy of protection. 311

III.

Since § 5.2 no. 11 of the North Rhine-Westphalia Constitution Protection Act is null and void as a whole, the complaints submitted against § 5.3 and § 17 of the North Rhine-Westphalia Constitution Protection Act are disposed of. Insofar as the complainants’ complaints are admissible, the unconstitutionality of the impugned provisions is claimed only with regard to measures according to the provision that is null and void. 312

IV.

§ 5a.1 of the North Rhine-Westphalia Constitution Protection Act is compatible with the Basic Law insofar as its area of application was expanded to cover activities within the meaning of § 3.1 no. 1 of the North Rhine-Westphalia Constitution Protection Act. In particular, this provision does not violate Article 2.1 in conjunction with Article 1.1 of the Basic Law. 313

1. The collection of account contents and account movements provided in § 5a.1 of the North Rhine-Westphalia Constitution Protection Act encroaches on the general right of personality in its manifestation as a right to informational self-determination. 314

Such account information can be significant for the protection of the personality of the person concerned, and is protected by the fundamental right. According to the current habits, most payment transactions which go beyond the cash transactions of daily life are carried out via accounts. If information is deliberately compiled on the contents of the accounts of a specific person, this makes it possible to view the assets and the social contacts of the person concerned, insofar as these show a financial dimension – for instance via subscriptions or maintenance payments. Some account content data, such as the amount of payments connected with consumption-dependent recurring obligations, can also permit further conclusions to be drawn as to the conduct of the person concerned (see Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2466)). 315

The measures provided in § 5a.1 of the North Rhine-Westphalia Constitution Protection Act encroach on the right to informational self-determination. It is not a matter here of whether the content of the impugned provision is limited to a power of the constitution protection authority to address a request for information to a financial institution, or whether it implicitly imposes an obligation on the respective financial institution to provide information. In either case, the provision empowers the authority to undertake data collection exercises which as such already bring about an encroachment on fundamental rights. 316

2. The encroachments on fundamental rights provided in § 5a.1 of the North Rhine-Westphalia Constitution Protection Act are however constitutionally justified for investigations in view of activities within the meaning of § 3.1 no. 1 of the North Rhine-Westphalia Constitution Protection Act. In particular, the impugned provision complies with the principle of proportionality in this respect. 317

a) Because of the expansion of the area of application of the provision, the measures regulated in § 5a.1 of the North Rhine-Westphalia Constitution Protection Act also serve the purpose of reconnaissance of the financing channels and of the financial circumstances and intertwinings in connection with activities within the meaning of § 3.1 no. 1 of the North Rhine-Westphalia Constitution Protection Act. This is a legitimate goal of protection of the constitution. 318

The provision in its expanded version is suited to reach this goal. It is also necessary for it. No equally effective means is evident to achieve reconnaissance of bank transactions with a view to activities within the meaning of § 3.1 no. 1 of the North Rhine-Westphalia Constitution Protection Act that is less burdening for the person concerned. 319

b) § 5a.1 of the North Rhine-Westphalia Constitution Protection Act also satisfies 320

the principle of appropriateness in the narrower sense.

aa) The provision empowers the constitution protection authority to effect encroachments on fundamental rights. 321

Information on account contents and account movements can be sensitive data the obtaining of knowledge of which considerably impairs the interests of the person concerned that are protected by fundamental rights. The collection of such information has hence as a rule an increased weight from the fundamental rights perspective (see Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2470)). The intensity of the encroachment is also increased by virtue of its secrecy. According to § 5a.3 sentence 11 of the North Rhine-Westphalia Constitution Protection Act, the financial institution which provides the information may not notify the person concerned of the request for information and of the data transmitted. Finally, the person concerned may incur disadvantages since the financial institution holding the account of necessity hears of the data collection and may draw unfavourable conclusions on an individual concerned on the basis of such knowledge (see Federal Constitutional Court, Order of 13 June 2007 – 1 BvR 1550/03 et al. –, *Neue Juristische Wochenschrift* 2007, p. 2464 (2469)). 322

bb) The public interests pursued with § 5a.1 of the North Rhine-Westphalia Constitution Protection Act are however so weighty that they are not disproportionate to the encroachments on fundamental rights that are regulated in the provision. 323

(1) The statute links the obtaining of knowledge on the account contents and account movements to factual preconditions which adequately accommodate the significance of the encroachment on fundamental rights for the person concerned. 324

§ 5a.1 of the North Rhine-Westphalia Constitution Protection Act makes the collection contingent on an element of endangerment that is qualified both as to the legal interests concerned, and as to the factual basis of the encroachment. There must be factual indications of grievous dangers to the interests protected contained in § 3.1 of the North Rhine-Westphalia Constitution Protection Act. The term “grievous danger” refers – as in § 8a.2 of the Federal Constitution Protection Act (*Bundesverfassungsschutzgesetz – BVerfSchG*) (see on this *Bundestag* document (*Bundestagsdrucksache – BTDrucks*) 16/2921, p. 14), which has identical wording in this respect – to an increased intensity of the threat to legal interests. The factual basis of the encroachments is additionally qualified by the requirement of factual indications of a grievous danger. It is not sufficient for the regulated data collection to be useful in general terms for the performance of the task of the constitution protection authority. Rather, indications must exist of a situation in which the protected interests are under threat in concrete terms. 325

With its two-fold qualification, the encroachment threshold meets the requirements of the general right of personality. No further restrictions of the factual preconditions of the encroachment are constitutionally required. 326

In particular, the view of the complainant re 1b that the substantive encroachment threshold must be increased as to the activities named in § 3.1 no. 1 of the North Rhine-Westphalia Constitution Protection Act such that § 5a.1 of the North Rhine-Westphalia Constitution Protection Act only covers activities that are militant and incite to hatred and violence is to be rejected. It is adequately ensured by the requirement of factual indications of a grievous danger that a vague suspicion that specific groups could target the free democratic fundamental order does not suffice to collect account contents and account movements. The concomitant encroachment, on the other hand, is not so grievous that it could only be proportionate for fighting violent groups or those groups which incite to hatred and violence. 327

No decisive constitutional objections emerge from the fact that § 5a.1 of the North Rhine-Westphalia Constitution Protection Act does not regulate any special requirements in the selection of the person concerned by data collection. On this basis, it may happen that account content data may be collected with regard to a person who is not under suspicion of being legally responsible for the danger. One can consider in particular that someone has been involved as a tool acting in good faith in asset transactions of the activities concerned. However, it is also constitutionally permissible to effect a measure according to § 5a.1 of the North Rhine-Westphalia Constitution Protection Act against such a person if it is otherwise impossible to clarify financing mechanisms. The selection between several conceivable persons concerned can also be adequately guided by the principle of proportionality that is applicable in the context of § 5a.1 of the North Rhine-Westphalia Constitution Protection Act. By contrast, information on the account contents of persons who are not under suspicion of being deliberately or non-deliberately involved in the asset transactions of the activities concerned will hardly ever be able to serve the statutory goal of countering a grievous danger by reconnaissance of financing mechanisms. 328

(2) The impugned provision also takes account of the grievousness of the regulated encroachment on fundamental rights by means of suitable procedural precautions. 329

For instance, data collection according to § 5a.3 sentence 3 of the North Rhine-Westphalia Constitution Protection Act requires an order from the Minister of the Interior, which is to be requested by the head of the constitution protection department or his or her deputy. The encroachment on fundamental rights lying in the collection of account contents and account movements is not so grievous that ex-ante control by a neutral body is constitutionally required per se. The intra-authority control provided however serves to secure the interests of the person concerned in the preparatory phase of data collection, and hence contributes to the proportionality of the encroachment. What is more, additional ex-post control by the G 10 Commission is provided for according to § 5a.3 sentences 4 to 8 of the North Rhine-Westphalia Constitution Protection Act, which equally serves the protection of the interests of the person concerned that are protected by fundamental rights. 330

§ 5a.3 sentence 9 of the North Rhine-Westphalia Constitution Protection Act in con- 331

junction with § 4 of the Act on the Implementation of the Act re Article 10 of the Basic Law contains standards for the processing and transmission of the collected data, in particular meeting the requirements of necessity and of the limitation principle.

§ 5a.3 sentence 11 of the North Rhine-Westphalia Constitution Protection Act in conjunction with § 5 of the Act on the Implementation of the Act re Article 10 of the Basic Law, finally, provides for notification of the person concerned as soon as a risk to the purpose of the restriction can be ruled out. By these means, the person concerned is largely enabled to pursue his or her interests at least ex post. 332

V.

The ruling on costs is based on § 34a.2 of the Federal Constitutional Court Act. 333

Papier Hohmann-Dennhardt Hoffmann-Riem

Papier	Hohmann-Dennhardt	Hofmann-Riem
Bryde	Gaier	Eichberger
Schluckebier		Kirchhof

Bundesverfassungsgericht, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07

Zitiervorschlag BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 - Rn. (1 - 333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html

ECLI ECLI:DE:BVerfG:2008:rs20080227.1bvr037007