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) encompasses the fundamental right to protection of the confidentiality and integrity of information technology systems.**

2. **The covert infiltration of an information technology system for the purposes of monitoring the use of the system and extracting data stored on its storage media is only permissible under constitutional law if there are factual indications of a specific danger to an exceptionally significant legal interest. Exceptionally significant legal interests are life, limb and liberty of the person or public interests that are of such significance that a threat to them would affect the foundations or existence of the state, or the foundations of human existence. The measure may be justified even if it cannot yet be established with sufficient probability that the danger will materialise in the near future, provided that there are specific facts indicating an impending danger to an exceptionally significant legal interest in the individual case that can be attributed to specific persons.**

3. **The covert infiltration of an information technology system in principle requires a judicial order. The statutory basis authorising such an interference must include safeguards to protect the core of private life.**

4. **To the extent that the legislative authorisation is limited to state measures intercepting the contents and circumstances of ongoing telecommunications in a computer network, or analysing data thus obtained, the interference must be measured against Article 10(1) of the Basic Law.**

5. **Where the state obtains knowledge of the contents of Internet communication by using the normal technical means provided for this purpose, an interference with Article 10(1) of the Basic Law arises only if the relevant state authority was not given permission to do so by one of the communicating parties.**

   Where the state obtains knowledge of communication contents that are publicly accessible on the Internet, or participates in publicly accessible communication processes, it generally does not interfere with fundamental rights.

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 370/07 -

- 1 BVR 595/07 -

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaint of

1. a) Ms W…,

b) Mr B….,

– authorised representative: …

against § 5(2) no. 11 in conjunction with § 7(1), § 5(3), § 5a(1) and § 13 of the North Rhine-Westphalia Constitution Protection Act as amended by the Act of 20 December 2006 (GVBl NRW 2006, p. 620)

- 1 BvR 370/07 -,

2. a) Mr B…,

b) Dr. R…,

c) Mr S…,

– authorised representatives: …

against § 5(2) no. 11, § 5(3), § 7(2) and § 8(4) second sentence in conjunction with §§ 10, 11 and § 17(1) of the North Rhine-Westphalia Constitution Protection Act as amended by the Act of 20 December 2006 (GVBl NRW 2006, p. 620)

- 1 BvR 595/07 -

the Federal Constitutional Court – First Senate –

with the participation of 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 North Rhine-Westphalia Constitution Protection Act as amended by the Act of 20 December 2006 (GVBl NRW, p. 620) is incompatible with Article 2(1) in conjunction with Article 1(1), Article 10(1) and Article 19(1) second sentence of the Basic Law, and thus void.**

2. **[…]**

3. **To the extent that it challenges § 5a(1) of the North Rhine-Westphalia Constitution Protection Act, the constitutional complaint of complainant no. 1b is rejected.**

4. **[…]**

5. **[…]**

REASONS:

A.

The constitutional complaints concern provisions of the NRW Constitution Protection Act that set out, firstly, the powers of the *Land* Office for the Protection of the Constitution (*Verfassungsschutzbehörde*) regarding various data collection measures, in particular the collection of data from information technology systems, and secondly, the processing of the collected data. 1

I.

[…] 2

1. Both constitutional complaints assert that § 5(2) no. 11 of the NRW Constitution Protection Act is unconstitutional. This provision authorises the *Land* Office for the Protection of the Constitution to carry out two types of investigation measures: covert monitoring and other Internet surveillance measures (first alternative), and covert access to information technology systems (second alternative). 3

a) […] Covert Internet surveillance is defined as a measure by which the *Land* Office for the Protection of the Constitution obtains knowledge of the contents of Inter- 4

net communication by using the normal technical means provided for this purpose. The *Land* Government of North Rhine-Westphalia refers to such measures as server-related Internet surveillance.

By contrast, covert accessing of an information technology system is defined as technical infiltration, for instance, by taking advantage of vulnerabilities in the target system's security or by installing spyware. The infiltration of the target system makes it possible to monitor its use, to access data on its storage media, and even to exercise remote control over the target system. The *Land* Government of North Rhine-Westphalia refers to such measures as client-related Internet surveillance. […] 5

b) […] 6

c) […] 7

aa) The challenged *Land* provision contains the first and so far the only explicit authorisation of a German state authority to carry out 'remote searches' of information technology systems. […] 8

bb) 'Remote searches' are designed to respond to the difficulties that arise in the context of criminal investigations where the perpetrators, especially those from extremist and terrorist groups, use information technology, in particular the Internet, for their communication and for the planning and committing of criminal acts. […] 9

[…] 10-11

d) […] 12

e) […] 13

2. […] 14

3. […] 15-16

4. […] 17

5. […] 18

6. […] 19

7. […] 20-115

II.

1. Complainant no. 1a is a journalist […]. In the context of her work, she visits websites operated by persons and organisations with anti-constitutional aims. She is also a data protection activist and, together with others, operates the website www.stop1984.com. This site allows users to participate in so-called chats; the chat service is also used by right-wing extremists. Complainant no. 1a stores information on chat participants on the hard drive of her computer, which she uses for both private and professional purposes. 116

Complainant no. 1b is an active member of the NRW regional branch of the party *DIE LINKE*, which is being monitored by the NRW Office for the Protection of the Constitution. He also uses his computer, which has Internet access, for his political activities. Like complainant no. 1a, he uses the Internet for private communication as well […]. 117

Complainants nos. 2a and 2b are partners in a law firm. Complainant no. 2a is a lawyer who *inter alia* represents asylum-seekers, including a leading member of the PKK, which is monitored by the NRW Office for the Protection of the Constitution. He uses computer networks that are connected to the Internet, both in his home and on the premises of the law firm. The law firm network is also used by complainant no. 2b, as well as by complainant no. 2c, who is a freelancer at the law firm. 118

2. To the extent that the constitutional complaints challenge § 5(2) no. 11 of the NRW Constitution Protection Act, the complainants claim a violation of Art. 2(1) in conjunction with Art. 1(1), Art. 10(1) and Art. 13(1) of the Basic Law. 119

[…] 120-122

3. […] 123

4. […] 124-125

5. […] 126-128

III.

The Federal Government, the *Land* Government and the *Land* Parliament of North Rhine-Westphalia, the Government of the Free State of Saxony, the Federal Officer for Data Protection and Freedom of Information and the Officer for Data Protection and Freedom of Information of the *Land* North Rhine-Westphalia submitted statements on the constitutional complaint. The parliamentary groups of *Sozialdemokratische Partei Deutschlands* (SPD) and *BÜNDNIS 90/DIE GRÜNEN* in the *Land* Parliament of North Rhine-Westphalia submitted a legal opinion. Furthermore, the Senate obtained written expert statements from Andreas Bogk, Dirk Fox, Professor Dr. Felix Freiling, Professor Dr. Andreas Pfitzmann and Professor Dr. Ulrich Sieber. 129

[…] 130-148

IV.

[…] 149

B.

[…] 150-164

C.

To the extent that they are admissible, the constitutional complaints are for the most part well-founded. § 5(2) no. 11 of the NRW Constitution Protection Act is unconstitutional and void regarding the second alternative listed there (see I below). The same applies to the first alternative listed in this provision (see II below). The fact that the provision is void renders moot the complaints directed against § 5(3) and § 17 of the NRW Constitution Protection Act (see III below). […] 165

I.

§ 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act, which governs the accessing of information technology systems, violates the general right of personality (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law) in its special manifestation as a fundamental right to protection of the confidentiality and integrity of information technology systems. 166

This manifestation of the general right of personality affords protection against the infiltration of information technology systems to the extent that protection is not already guaranteed by other fundamental rights, such as Art. 10 or Art. 13 of the Basic Law, nor by the right to informational self-determination (see 1 below). In the case at hand, the interferences are not justified under constitutional law: § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act satisfies neither the requirement of legal clarity (see 2 a below), nor the requirements deriving from the principle of proportionality (see 2 b below), nor does the provision set out sufficient safeguards protecting the core of private life (see 2 c below). The challenged provision is thus void (see 2 d below). There is no need for further review of the provision based on other fundamental rights (see 2 e below). 167

1. § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act authorises interferences with the general right of personality in its special manifestation as a fundamental right to protection of the confidentiality and integrity of information technology systems; this manifestation supplements other specific manifestations of that fundamental right such as the right to informational self-determination, as well as the freedoms guaranteed in Art. 10 and Art. 13 of the Basic Law in cases where these do not afford sufficient protection. 168

a) The general right of personality protects aspects of one’s personality that are not covered by the specific freedoms of the Basic Law, but are equal to these freedoms in terms of their constitutive significance for one’s personality (cf. BVerfGE 99, 185 <193>; 114, 339 <346>). Such a guarantee that fills gaps in protection is in particular necessary in order to respond to new risks [to one’s personality], which possibly arise in the context of scientific and technical progress or societal change (cf. BVerfGE 54, 148 <153>; 65, 1 <41>; 118, 168 <183>). Determining what specific legal protection is invoked in relation to the various manifestations of the right of personality is mainly informed by the type of risk to one’s personality at play (cf. BVerfGE 101, 361 <380>; 169

106, 28 <39>).

b) The use of information technology has taken on an unprecedented significance for the personality and development of the individual. Modern information technology opens up new opportunities for individuals, but also creates new risks to one's personality. 170

aa) Recent developments in information technology have led to a situation in which information technology systems have become ubiquitous, and their use central to the lives of many people. 171

This applies first and foremost to personal computers, which can now be found in a large majority of households in the Federal Republic of Germany […]. The performance of such computers has increased, as has the capacity of their internal memories and their storage media. Today's personal computers can be used for many different purposes […]. Accordingly, the significance of personal computers for the development of one's personality has increased considerably. 172

[…] Additionally, many devices used everyday by large parts of the population involve information technology components. This is increasingly true with regard to telecommunication or electronic devices in homes or motor vehicles, for instance. 173

bb) The functions of information technology systems and their significance for the development of one's personality are amplified where different systems are connected. This is increasingly becoming the norm, not least due to the increase in Internet usage by large parts of the population. 174

[…] 175

Most notably, the Internet, as a complex structure linking computer networks, not only provides users of connected computers with access to a virtually limitless wealth of information that is made available by and can be retrieved from other network computers. On the Internet, users have access to numerous innovative communication services, too, allowing them to actively establish and maintain social relations. […] 176

cc) The increasingly widespread use of networked information technology systems provides individuals with new opportunities for personality development, but also creates new risks to their personality. 177

(1) These risks arise because complex information technology systems such as personal computers allow for a wide range of possible uses, all of which entail the creation, processing and storage of data. This concerns not only data which computer users create or store deliberately. In the context of data processing, information technology systems autonomously create large quantities of further data which, like the data stored by users, can be analysed to determine user behaviour and characteristics. As a consequence, a large amount of data relating to users' personal circumstances, social contacts and activities can be accessed in the working memory and the storage media of such systems. If collected and analysed by third parties, this 178

data allows for far-reaching conclusions regarding the personality of the users concerned, and may even make it possible to compile personality profiles (cf. regarding the risks to one's personality from such findings BVerfGE 65, 1 <42>).

(2) In a networked system, in particular one connected to the Internet, these risks are aggravated in various ways. Firstly, the network connection expands the possible areas of use, leading to the creation, processing and storage of even larger and more diverse amounts of data in comparison to a stand-alone system. This includes communication contents, as well as data relating to network communication. Extensive knowledge about users' personalities can be obtained by way of storing and analysing data on user behaviour in the network. 179

Above all, the system's network connection gives third parties the technical ability to access it, including for the purposes of spying on or manipulating data stored in the system. Individuals will not always be able to detect such third-party access; in any case, they have only limited powers to prevent it. Information technology systems have now evolved to such complexity that taking effective social or technical measures of self-protection presents a considerable challenge and may not be feasible at least for the average user. […] 180

c) From a fundamental rights perspective, a considerable need for protection arises given that the use of information technology systems has significance for one's personality development but also entails risks to one's personality. For the sake of the unimpeded development of one's personality, individuals have legitimate expectations regarding the integrity and confidentiality of such systems, and they rely on the state to respect these expectations. The guarantees of Art. 10 and Art. 13 of the Basic Law, like the manifestations of the general right of personality previously developed by the Federal Constitutional Court in its case-law, do not adequately take account of the need for protection arising from advances in information technology. 181

aa) The guarantee of telecommunications privacy under Art. 10(1) of the Basic Law protects the non-physical transmission of information to individual recipients by way of telecommunications traffic (cf. BVerfGE 67, 157 <172>; 106, 28 <35 and 36>); yet its protection does not extend to the confidentiality and integrity of information technology systems. 182

(1) The protection under Art. 10(1) of the Basic Law covers telecommunications, regardless of the method of transmission (cable or wireless, analogue or digital) and the form of expression (speech, images, sound, symbols or other data) used (cf. BVerfGE 106, 28 <36>; 115, 166 <182>). The scope of protection of telecommunications privacy thus also extends to Internet communication services (cf. regarding emails BVerfGE 113, 348 <383>). What is more, not only the actual communication contents, but also the circumstances of telecommunications are protected against the state obtaining knowledge thereof. This includes in particular whether, when and how often telecommunication traffic occurred or was attempted between whom or between which telecommunication devices (cf. BVerfGE 67, 157 <172>; 85, 386 <396>; 183

100, 313 <358>; 107, 299 <312 and 313>). In this context, the privacy of telecommunications is faced with both old and new risks to one's personality arising from the increased significance of information technology for the personal development of the individual.

Where a legislative authorisation is limited to state measures intercepting the contents and circumstances of ongoing telecommunications in a computer network, or to measures analysing this data, the interference must be measured only against Art. 10(1) of the Basic Law. In this case, the scope of protection of this fundamental right is affected regardless of whether, at the technical level, the measure targets the transmission route or the device used for telecommunications (cf. BVerfGE 106, 28 <37 and 38>; 115, 166 <186 and 187>). In principle, this also applies if the device is a networked and complex information technology system that is used for telecommunications but also for various other types of activities. 184

(2) Yet the fundamental rights protection afforded by Article 10(1) of the Basic Law does not extend to the contents and circumstances of telecommunications data stored within the domain controlled by a communicating party after the transmission has been completed, to the extent that they can take their own precautions against covert data access. Regarding such data, the specific risks of remote communication, which the privacy of telecommunications aims to avert, no longer apply (cf. BVerfGE 115, 166 <183 *et seq.*>). 185

(3) Likewise, the protection afforded by the privacy of telecommunications does not apply if a state authority monitors the use of an information technology system as such or searches the system's storage media. […] 186

(4) To the extent that covert access to an information technology system serves to also collect data not protected by Art. 10(1) of the Basic Law, a gap in protection arises, which must be filled by the general right of personality in its manifestation as protection of the confidentiality and integrity of information technology systems. 187

Where the technical infiltration of a complex information technology system is undertaken for the purposes of telecommunications surveillance ('source telecommunications surveillance'), this infiltration is the critical step that makes it possible to spy on the system as a whole. The resulting risks [for one's personality] go far beyond the risks associated with the mere surveillance of ongoing telecommunications. […] 188

[…] 189

By contrast, Art. 10(1) of the Basic Law serves as the sole standard of review in terms of fundamental rights protection where the authorisation to carry out 'source telecommunications surveillance' is strictly limited to data stemming from ongoing telecommunications. This must be ensured by technical and legal safeguards. 190

bb) The right to the inviolability of the home afforded by Art. 13(1) of the Basic Law guarantees individuals an essential space of private life in light of human dignity and 191

for the development of their personality, where interferences are only permissible subject to the particular requirements set out in Art. 13(2) to 13(7) of the Basic Law; however, it leaves gaps in protection as regards access to information technology systems.

This fundamental right protects the sphere of private space within one's home, in which private life unfolds (cf. BVerfGE 89, 1 <12>; 103, 142 <150 and 151>). In addition to private homes, commercial and business premises are also covered by the scope of protection of Art. 13 of the Basic Law (cf. BVerfGE 32, 54 <69 *et seq*.>; 44, 353 <371>; 76, 83 <88>; 96, 44 <51>). The fundamental rights protection is not limited to preventing physical intrusions into the home. Measures that entail the use of technical equipment by state authorities for the purposes of obtaining insights into activities within homes that cannot be naturally perceived from outside the protected space must also be regarded as interferences with Art. 13 of the Basic Law. […] 192

[…] 193

However, Art. 13(1) of the Basic Law does not generally protect individuals against any infiltration of their information technology system regardless of how the accessing is carried out, not even if the system is located within a private home […]. The interference at issue can occur regardless of one's location; therefore, a location-specific protection could not counter the specific risks to the information technology system. To the extent that infiltration measures make use of a network connection between the targeted computer and another computer, they do not affect the sphere of private space within one's home. In many cases, the location of the targeted system is irrelevant for the investigation measure, and will frequently not even be known to the authority. This applies in particular to mobile information technology systems such as laptops, personal digital assistants or mobile phones. 194

Nor does Art. 13(1) of the Basic Law afford protection against the collection, by means of system infiltration, of data from the working memory or storage media of an information technology system located within a private home (cf. regarding the equivalence of protection applicable in relation to home searches and seizing of evidence BVerfGE 113, 29 <45>). 195

cc) The manifestations of the general right of personality that have previously been recognised in the Federal Constitutional Court's case-law, in particular the guarantees protecting the private sphere and the right to informational self-determination, also do not sufficiently meet the special need for protection of users of information technology systems. 196

(1) In its manifestation as protection of the private sphere, the general right of personality guarantees individuals a [protected] domain tied to certain spaces or subject matters which is to remain, in principle, free of unwanted scrutiny (cf. BVerfGE 27, 344 <350 *et seq.*>; 44, 353 <372 and 373>; 90, 255 <260>; 101, 361 <382 and 383>). However, the need for protection on the part of users of information technology sys- 197

tems is not limited solely to data attributable to their private sphere. […]

(2) The scope of the right to informational self-determination goes beyond the protection of the private sphere. It confers upon the individual the authority to, in principle, decide themselves on the disclosure and use of their personal data (cf. BVerfGE 65, 1 <43>; 84, 192 <194>). It complements and expands the fundamental rights protection afforded freedom of conduct and private life, ensuring that this protection can be invoked against risks to one's personality. Such a risk can already arise before specific threats to identifiable legal interests materialise; this applies in particular where personal information can be used and linked in a manner which the person concerned can neither foresee nor prevent. In this context, the scope of protection of the right to informational self-determination is not limited to information that merits fundamental rights protection simply by virtue of its sensitive nature. Depending on the aims pursued by the accessing of data, and in light of the existing possibilities with regard to the processing and linking of data, the use of personal data which by itself has only little informative value may nevertheless affect the private life and freedom of conduct of the person concerned in a manner that is significant from a fundamental rights perspective (cf. BVerfGE 118, 168 <185>). 198

Risks to one's personality that the right to informational self-determination aims to avert arise from the manifold possibilities for the state, and in some cases also private actors, […] to collect, process and use personal data. By means of electronic data processing in particular, such information may be used to generate further information; this allows conclusions to be drawn, which may both impair the confidentiality interests of affected persons that are protected by fundamental rights and interfere with their freedom of conduct (cf. BVerfGE 65, 1 <42>; 113, 29 <45 and 46>; 115, 320 <342>; 118, 168 <184 and 185>). 199

However, the right to informational self-determination does not fully account for risks to one's personality arising from the fact that individuals rely on the use of information technology systems for the development of their personality, entrusting the system with personal data or inevitably generating such data simply by using the system. Third parties accessing the system can potentially obtain extremely large quantities of data with significant informative value without having to resort to further data collection and processing measures. The weight of such data access for the personality of affected persons goes far beyond that of isolated data collection measures against which the right to informational self-determination affords protection. 200

d) To the extent that no adequate protection exists against risks to one's personality arising from the fact that individuals rely on the use of information technology systems for their personality development, the general right of personality applies by virtue of its function to fill gaps in protection; it meets the aforementioned need for protection, which goes beyond the other manifestations of this right recognised so far, by guaranteeing the integrity and confidentiality of information technology systems. This right, just like the right to informational self-determination, is based on Art. 2(1) in 201

conjunction with Art. 1(1) of the Basic Law; it protects the personal and private life of fundamental rights holders against state access in the area of information technology; this protection is not limited to cases where the access concerns individual communication processes or selected stored data, but also applies where access to the information technology system as a whole is concerned.

aa) […] 202

The fundamental right to protection of the integrity and confidentiality of information technology systems is applicable where the statutory basis authorising interferences covers systems that may contain, by themselves or due to network connections, personal data of users in such large quantities and of such variety that access to the system facilitates insights into essential aspects of one's personal life or even allows for the creation of a comprehensive personality profile. These possibilities exist, for instance, when personal computers are accessed, regardless of whether they are installed in a fixed location or operated as mobile devices. Regarding both private and business computer use, usage patterns regularly allow conclusions to be drawn regarding personal characteristics or preferences. In addition, the specific fundamental rights protection also covers such mobile phones or electronic assistants that offer a wide range of functions and can collect and store various kinds of personal data. 203

bb) The fundamental right to protection of the confidentiality and integrity of information technology systems primarily protects the user's interest in confidentiality of the data created, processed and stored by information technology systems that falls within its scope of protection. Moreover, it constitutes an interference with this fundamental right if the integrity of the protected information technology system is compromised because the system is accessed in a manner that allows third parties to use its services, functions and storage contents; such access is the critical technical step that enables spying, monitoring or manipulation activities in relation to this system. 204

(1) In its manifestation addressed here, the general right of personality affords protection particularly against covert access through which data available in the system can be spied on in its entirety or on a large scale. This fundamental rights protection extends to both the data stored in the working memory and the data temporarily or permanently kept on the system's storage media. The fundamental right also protects against data collection carried out by means that, even though they are not directly connected at a technical level to the data processing activities of the information technology system in question, nevertheless pertain to the system's data processing. This applies, for example, to the use of so-called hardware keyloggers or to the measuring of electromagnetic radiation from monitors or keyboards. 205

(2) The expectation of confidentiality and integrity is afforded fundamental rights protection regardless of whether the information technology system can be accessed easily or only with considerable effort. Yet the expectation of confidentiality and integrity is recognised from a fundamental rights perspective only insofar as the affected user regards the information technology system as their own system, so that they 206

can legitimately expect that, based on the relevant circumstances, they have control over the information technology system in a self-determined manner, either alone or together with other authorised users of the system. […]

2. The fundamental right to protection of the confidentiality and integrity of information technology systems is not guaranteed without limitation. Interferences may be justified both for preventing [dangers to public security] and for law enforcement purposes. Individuals must only accept such restrictions of their right that have a statutory basis in line with constitutional law. The provision authorising the *Land* Office for the Protection of the Constitution to carry out preventive measures, which is under review in the present proceedings, does not satisfy this requirement. 207

a) The provision at issue does not meet the requirement of legal clarity and specificity. 208

aa) The requirement of legal specificity is based on the principle of the rule of law (Art. 20 and Art. 28(1) of the Basic Law), including where it concerns the general right of personality in its various manifestations (cf. BVerfGE 110, 33 <53, 57, 70>; 112, 284 <301>; 113, 348 <375>; 115, 320 <365>). It serves to ensure that the parliamentary legislator, which is democratically legitimated, takes the essential decisions on interferences with fundamental rights and their scope itself; that the law subjects the government and administration to standards that direct and limit their actions; and that the courts can review the lawfulness of their actions. Furthermore, clear and specific provisions ensure that affected persons are able to discern the applicable law and can take precautions against potentially intrusive measures (cf. BVerfGE 110, 33 <52 *et seq.*>; 113, 348 <375 *et seq.*>). The legislator must specify, in a sufficiently clear and precise manner and for each subject matter, the grounds, purpose and limits of the interference (cf. BVerfGE 100, 313 <359 and 360, 372>; 110, 33 <53>; 113, 348 <375>; 118, 168 <186 and 187>). 209

[…] 210

bb) Based on these standards, § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act does not satisfy the requirement of legal clarity and specificity insofar as the conditions under which the measures are permissible cannot be derived from the statutory provision with sufficient certainty. 211

(1) The statutory conditions for carrying out measures pursuant to § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act are determined by two references to other provisions. Firstly, § 5(2) of the NRW Constitution Protection Act contains a general reference to § 7(1) of the NRW Constitution Protection Act, which in turn refers to § 3(1) of the NRW Constitution Protection Act. These provisions authorise the use of intelligence service methods for the purposes of gathering information relevant to the protection of the constitutional order. Secondly, § 5(2) no. 11 second sentence of the NRW Constitution Protection Act refers to the more stringent requirements set out in the Act on Article 10 of the Basic Law (hereinafter: 212

the Article 10 Act) for cases in which a measure pursuant to § 5(2) no. 11 of the NRW Constitution Protection Act interferes with the privacy of correspondence, post and telecommunications or is equivalent to such an interference due to its nature and severity.

(2) It is not compatible with the requirement of legal clarity and specificity that § 5(2) no. 11 second sentence of the NRW Constitution Protection Act makes the applicability of the Article 10 Act contingent on whether a measure interferes with Art. 10 of the Basic Law. […] The legislative use of a fall-back clause (*salvatorische Klausel*) does not satisfy the requirement of legal specificity for a provision such as § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act, which provides for novel investigation measures designed in response to new technological developments. 213

The violation of the requirement of legal clarity is further aggravated by § 5(2) no. 11 second sentence of the NRW Constitution Protection Act, which additionally states that the Article 10 Act also applies if the "nature and severity" of an investigation measure is equivalent to an interference with Art. 10 of the Basic Law. Hence, the conditions under which the accessing [of information technology systems] pursuant to the challenged provision is permissible are contingent upon an assessment comparing the accessing measure to a measure that would qualify as an interference with a specific fundamental right. § 5(2) no. 11 second sentence of the NRW Constitution Protection Act completely lacks any criteria for undertaking such a comparison. […] 214

(3) Furthermore, the reference to the Article 10 Act in § 5(2) no. 11 second sentence of the NRW Constitution Protection Act fails to satisfy the requirement of legal clarity and specificity insofar as its scope is not sufficiently clear. 215

[…] 216-217

b) § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act also fails to satisfy the principle of proportionality. This principle requires that an interference with fundamental rights serve a legitimate purpose and be suitable, necessary and appropriate for achieving this purpose (cf. BVerfGE 109, 279 <335 *et seq.*>; 115, 320 <345>; 118, 168 <193>; established case-law). 218

aa) The data collection measures provided for in the challenged provision are designed to aid the *Land* Office for the Protection of the Constitution in fulfilling its tasks […], and thus serve to protect, as precautionary measures before specific dangers (*konkrete Gefahren*) arise, the free democratic basic order, the existence of the Federation and of the *Länder*, as well as interests of the Federal Republic of Germany that concern its international relations. […] 219

The security of the state as a constituted power of peace and order, as well as the security of the population it is bound to protect against dangers to life, limb and liberty, rank equally with other constitutional values that are accorded high standing (cf. BVerfGE 49, 24 <56 and 57>; 115, 320 <346>*)*. The [state's] duty of protection fol- 220

lows from both Art. 2(2) first sentence and Art. 1(1) second sentence of the Basic Law (cf. BVerfGE 115, 118 <152>). In countering dangers from terrorist or other activities, the state fulfils its constitutional mandate. The increased use of electronic or digital means of communication and their advance into virtually all areas of life has created new obstacles for the effective performance of the tasks of the Office for the Protection of the Constitution. Modern information technology also offers extremist and terrorist groups numerous possibilities to establish and maintain contacts, as well as to plan, prepare and commit criminal acts. In particular, legislative measures that allow state investigations to target information technology must be considered against the background of the shift from traditional forms of communication to electronic messaging and the possibilities to encrypt or conceal data files (cf. regarding law enforcement BVerfGE 115, 166 <193>).

bb) The covert accessing of information technology systems is suitable for achieving these purposes. It expands the possibilities available to the *Land* Office for the Protection of the Constitution to investigate threats. The legislator is granted a considerable margin of appreciation in assessing the suitability of a measure (cf. BVerfGE 77, 84 <106>; 90, 145 <173>; 109, 279 <336>). […] 221

[…] 222-223

cc) Moreover, the covert accessing of information technology systems does not violate the requirement of necessity. It was within the legislator's prerogative of assessment to presume that other means for the collection of data from information technology system that would be equally effective but less intrusive for the affected persons are not available. 224

[…] 225

dd) However, § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act does not satisfy the requirement of proportionality in the strict sense. 226

The principle of proportionality in its strict sense requires that the severity of the interference, in an overall assessment, not be disproportionate to the weight of the reasons invoked to justify it (cf. BVerfGE 90, 145 <173>; 109, 279 <349 *et seq.*>; 113, 348 <382>; established case-law). The legislator must appropriately weigh the individual's interest that is curtailed by an interference with fundamental rights against the public interests pursued. An assessment based on these standards may lead to the conclusion that certain means must not be used to enforce public interests because the resulting impairments of fundamental rights outweigh the interests pursued (cf. BVerfGE 115, 320 <345 and 346>; 118, 168 <195>). 227

§ 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act does not satisfy this requirement. The measures set out in that provision result in fundamental rights interferences that are so serious that they are disproportionate to the public investigation interest providing the grounds for interference. Moreover, ad- 228

ditional procedural safeguards would be necessary to give effect to the protected fundamental rights interests of affected persons; these are also lacking in the provision.

(1) § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act authorises particularly intrusive interferences with fundamental rights. 229

(a) Where the state collects data from complex information technology systems, there is a considerable potential that the data might be used to spy on the personality of the affected persons. This already applies to measures that only entail one-off and isolated access, such as the seizure or copying of the system's storage media (cf. in this regard BVerfGE 113, 29; 115, 166; 117, 244). 230

(aa) Such covert accessing of information technology systems provides the relevant state authority with access to data records which, in terms of their volume and variety, may by far exceed traditional sources of information. This follows from the fact that complex information technology systems allow for many different possible uses which entail the creation, processing and storage of personal data. In light of today's user habits, such devices are typically also used to deliberately store personal data that is particularly sensitive, for example private text documents, images or sound files. These data records may include detailed information on the personal circumstances and private life of the affected person, their private and business correspondence via various communication channels, or even diary-like personal notes. 231

State access to such comprehensive data records entails the obvious risk that, in an overall assessment, the collected data allows comprehensive conclusions to be drawn regarding the personality of the affected person, which may even include the creation of behaviour and communication profiles. 232

(bb) To the extent that the collected data provides information on communications between the affected person and third parties, the severity of the interference with fundamental rights is aggravated further given that it restricts the freedom of citizens to participate in telecommunications without being monitored – a freedom that also serves the common good […]. In addition, such data collection measures indiscriminately affect a considerable number of persons, which increases the weight of interference, since they necessarily also concern the target person's communication partners, i.e. third parties, regardless of whether the statutory grounds for such data access are also met in relation to these third parties (cf. regarding telecommunications surveillance BVerfGE 113, 348 <382 and 383>; furthermore BVerfGE 34, 238 <247; 107, 299 <321>). 233

(b) The interference with fundamental rights is particularly serious if – as provided for by the challenged provision – covert technical infiltration allows for longer-term surveillance of system use and the ongoing collection of the relevant data. 234

(aa) The volume and variety of the data records which can be obtained by such access are considerably higher than in case of one-off, isolated data collection measures. In accessing the target system, the investigating authority also obtains volatile 235

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 affected person over a longer period. Moreover, the indiscriminate effects of the investigation measure can increase if access is extended to a (local) network that the target system is part of.

Volatile data or data stored only temporarily can have particularly close links to the personality of affected persons; it can also facilitate access to further, especially sensitive data. This applies for instance to cache data, which is created by software applications such as web browsers; its analysis can provide information on how such applications are used, and may thus indirectly allow conclusions to be drawn on users' preferences or communication patterns. It also holds true for passwords, which allow the user to gain access to technically secure contents on their system or the network. Furthermore, longer-term surveillance of Internet communication, as authorised by the challenged provision, is a considerably more intrusive interference than a one-off collection of data on communication contents and circumstances. Finally, it must be taken into consideration that the possibilities of access set out in the challenged provision serve *inter alia* to circumvent the use of encryption technology and constitute suitable means in this regard. Thus, the individual precautions taken by users to protect themselves against unwanted data access are undermined. The frustration of informational self-protection undertaken by affected persons increases the severity of the interference with their fundamental rights. 236

In addition, there is an increased risk that this will lead to the creation of behaviour and communication profiles given that the provision authorises the comprehensive monitoring of the target system's usage over a longer period. By these means, the competent state authority can extensively spy on the personal circumstances and communication behaviour of affected persons. Such comprehensive collection of personal data amounts to a particularly intrusive interference with fundamental rights. 237

(bb) The severity of the interference stemming from the accessing [of information technology systems] as set out in the Act follows furthermore from the covert nature of the measure. In a state under the rule of law, state interferences through covert measures are the exception and require special justification (cf. BVerfGE 118, 168 <197>). If the persons concerned know about a state measure affecting them prior to its execution, they can defend their interests from the outset. Firstly, they can take legal steps to prevent it, for instance by seeking recourse to a court. Secondly, where data collection measures are carried out overtly, they can actually influence the course of the investigation with their conduct. Excluding this possibility to influence the investigation increases the weight of the interference with fundamental rights (cf. regarding possibilities of legal defence BVerfGE 113, 348 <383 and 384>; 115, 320 <353>). 238

(cc) The weight of the interference is also informed by possible risks to the integrity of the accessed computer and to legal interests of the persons concerned, or even of 239

third parties, that may result from such access.

[…] 240-241

(2) In view of its severity, the interference with fundamental rights stemming from the covert accessing of information technology systems for prevention purposes is only appropriate if specific facts indicate an impending danger (*drohende Gefahr*) to an exceptionally significant legal interest in the individual case; this requirement can be satisfied even if it cannot yet be established with sufficient probability that the danger will materialise in the near future. In addition, the statutory provision authorising such an interference must ensure that the fundamental rights of affected persons are protected, including by suitable procedural safeguards. 242

(a) With regard to the tension between the state's duty to guarantee the protection of legal interests and the interest of the individual in upholding their constitutionally guaranteed rights, it is primarily incumbent on the legislator to achieve an abstract balance between the conflicting interests (cf. BVerfGE 109, 279 <350>). As a result, certain particularly intrusive interferences with fundamental rights may only be permissible for the protection of certain legal interests and only when the suspicion or danger prompting the interference reaches a certain threshold. The state's duty to protect other legal interests is further limited by the prohibition of inappropriate interferences with fundamental rights (cf. BVerfGE 115, 320 <358>). The relevant thresholds for carrying out the measures constituting interferences must be set out in statutory provisions (cf. BVerfGE 100, 313 <383 and 384>; 109, 279 <350 *et seq.*>; 115, 320 <346>). 243

(b) Where the interference with fundamental rights is particularly intrusive, the measure may already be disproportionate as such if the grounds for interference set out in its statutory basis are not sufficiently weighty. To the extent that the applicable law serves to avert certain dangers, as is the case here according to § 1 of the NRW Constitution Protection Act, the significance and the nature of the threat to protected interests that the respective provision refers to are essential for determining the weight attached to the grounds for interference (cf. BVerfGE 115, 320 <360 and 361>). 244

If the interests that the statutory provision authorising interferences aims to protect are as such sufficiently weighty to justify interferences with fundamental rights of that type, the principle of proportionality gives rise to further constitutional requirements regarding the statutory basis, which set the prerequisites for interference. In this respect, the legislator must maintain a balance between the type and severity of the fundamental rights impairment on the one hand and the statutory prerequisites for carrying out the measures constituting interferences on the other hand (cf. BVerfGE 100, 313 <392 *et seq.*>). The statutory requirements pertaining to the necessary degree of probability and the factual basis of the prognosis must be proportionate to the type and intensity of the resulting impairment of fundamental rights. Even where the threats the interference aims to avert concern exceptionally weighty legal interests, 245

the requirement of sufficient probability cannot be dispensed with. In addition, the statutory basis must subject any serious interference with fundamental rights to the requirement that the assumptions and conclusions prompting the interference be based on specific facts (cf. BVerfGE 113, 348 <386>; 115, 320 <360 and 361>).

(c) The principle of proportionality sets limits for a statutory provision authorising covert access to information technology systems insofar as it gives rise to special requirements regarding the grounds for interference. […] 246

(aa) Such an interference may only be authorised if the statutory basis makes it contingent upon the existence of factual indications of a specific danger to an exceptionally significant legal interest. Such exceptionally significant legal interests primarily include life, limb and liberty of the person. They also include public interests that are of such significance that a threat to them would affect the foundations or existence of the state, or the foundations of human existence. These include, for instance, the functioning of essential and vital public infrastructure. 247

For the protection of other legal interests, […] state measures must be limited to the existing investigatory powers conferred for prevention purposes in the respective field of law. 248

(bb) As a prerequisite for covert access, the statutory basis must also require that there be at least certain factual indications of a specific danger to the sufficiently weighty protected interests set out in the relevant provision. 249

03b1) Given the requirement of factual indications, mere assumptions or conclusions drawn from general experience are by themselves not sufficient to justify covert access. Rather, specific facts must be established that support a prognosis of danger (cf. BVerfGE 110, 33 <61>; 113, 348 <378>). 250

This prognosis must point to the existence of a specific danger. This means that there must be a factual situation where it is sufficiently likely, in the individual case, that certain persons will cause damage to the interests protected by the relevant statutory provision in the foreseeable future, unless the state intervenes. The existence of a specific danger is determined by three criteria: it concerns an individual case; it is foreseeable that the danger will result in actual damage within a certain period of time; and the cause of the danger can be attributed to individual persons. However, the accessing of information technology systems at issue here may already be justified at a time when it cannot be established with sufficient probability that the danger will materialise in the near future, provided that there are already specific facts indicating an impending danger in the individual case with regard to an exceptionally significant legal interest. Firstly, it must at least be possible to determine, based on these facts, the type of incident that might occur, and that it will occur within a foreseeable timeframe; secondly, the facts must indicate the involvement of specific persons whose identity is known at least to such an extent that the surveillance measures can be targeted at and for the most part limited to them. 251

By contrast, the weight of interference resulting from covert access to an information technology system is not sufficiently taken into account where statutory provisions authorise the measure on grounds so precautionary in nature that the existence of a specific danger to the protected legal interests need no longer be foreseeable at all, not even with regard to its basic characteristics. 252

[…] 253

03b2) Regarding the covert accessing of information technology systems, the constitutional requirements relating to the factual grounds prompting the interference apply to all instances where statutory provisions authorise interferences with fundamental rights that serve the aim of preventing dangers. Since in all these instances, the impairment resulting from the interference for the affected persons is the same, there is no need to set different requirements for different authorities, for instance by differentiating between police authorities and other authorities entrusted with preventive tasks such as offices for the protection of the Constitution. For the purposes of weighing the covert accessing of information technology systems, it is in principle irrelevant that the police and offices for the protection of the Constitution have different responsibilities and powers, and that, in consequence, the depth of interference resulting from their measures may differ. 254

[…] 255-256

(d) Furthermore, statutory provisions authorising the covert accessing of information technology systems must provide for suitable procedural safeguards protecting the interests of the affected persons. […] In particular, such accessing must generally be subject to judicial authorisation. 257

(aa) The requirement of judicial authorisation allows for prior review of a planned covert investigation measure by an independent and neutral authority, which may significantly contribute to effective fundamental rights protection. […] 258

(bb) If a covert investigation measure involves a serious interference with fundamental rights, prior review by an independent authority is constitutionally required because the affected person would otherwise not be afforded any protection. […] 259

The legislator may only entrust a non-judicial authority with exercising this oversight if that authority guarantees the same level of independence and neutrality as a judge. When deciding on the lawfulness of the covert measure, such an oversight authority is also required to state reasons for its decision. 260

This requirement of prior review by a suitable neutral authority may exceptionally be dispensed with in urgent cases, for instance in cases of danger requiring immediate action (*Gefahr im Verzug*); yet it must be ensured that in these cases the neutral authority will conduct an *ex post* review of the measure. In this context, a finding of urgency must meet certain factual and legal conditions informed by constitutional law (cf. BVerfGE 103, 142 <153 *et seq.*> regarding Art. 13(2) of the Basic Law). 261

(3) Based on these standards, the challenged provision does not satisfy the constitutional requirements. 262

(a) According to § 5(2) in conjunction with § 7(1) no. 1 and § 3(1) of the NRW Constitution Protection Act, the use of intelligence service methods by the *Land* Office for the Protection of the Constitution is only subject to the condition that there are factual indications suggesting that these methods allow the gathering of information on anti-constitutional activities. This does not subject the exercise of these powers to a sufficient substantive threshold, neither regarding the factual conditions for carrying out the interference, nor regarding the weight of the legal interests the measure aims to protect. Also, the provision fails to ensure prior review by an independent authority, so that the constitutionally required procedural safeguards are lacking. 263

(b) These shortcomings are not remedied, not even when taking into account – despite its lack of legal specificity – the statutory reference in § 5(2) no. 11 second sentence of the NRW Constitution Protection Act to the more detailed requirements for surveillance measures under the Article 10 Act, and when interpreting this reference broadly, as suggested by the *Land* Government of North Rhine-Westphalia, to the effect that it renders applicable all formal and substantive safeguards set out in the Article 10 Act. While § 3(1) of the Article 10 Act does set out conditions for the use of telecommunications surveillance, covert access to an information technology system pursuant to § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act is not limited to telecommunications surveillance; rather, the provision generally allows covert access for obtaining all available data from an information technology system. 264

The grounds for interference set out in § 3(1) of the Article 10 Act do not satisfy the constitutional requirements, neither with regard to the threshold for exercising the relevant powers nor with regard to procedural safeguards. 265

(aa) Under § 3(1) first sentence of the Article 10 Act, surveillance measures are permissible if there are factual indications supporting the suspicion that someone is planning, committing or has committed a criminal offence listed in the catalogue set out in that provision. Firstly, the catalogue of criminal offences does not appear to be informed by an overall concept under which all the criminal offences listed in that catalogue would constitute sufficient grounds that could justify measures pursuant to § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act. Therefore, not all statutory grounds under the Article 10 Act that the challenged provision refers to ensure that the accessing [of information technology systems] in the specific case actually serves to protect one of the aforementioned exceptionally significant legal interests […]. Secondly, the reference to § 3(1) first sentence of the Article 10 Act does not ensure in each case that the covert accessing of information technology systems takes place only if it can be presumed with sufficient probability that relevant legal interests will be endangered […] in the near future. 266

[…] 267

(bb) § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act does not meet the constitutional requirements regarding prior review of covert access to an information technology system, not even when taking into account the reference to the Article 10 Act. 268

§ 10 of the Article 10 Act provides that surveillance measures must be authorised by an order issued by the competent *Land* ministry upon request by the *Land* Office for the Protection of the Constitution. This procedure is not sufficient to ensure the prior review required by Art. 2(1) in conjunction with Art. 1(1) of the Basic Law. The foregoing provision sets out neither a requirement of judicial authorisation, nor – given that the prior review exercised by the Article 10 Committee (*G 10-Kommission*) according to § 3(6) of the Act on the Implementation of the Article 10 Act is not included in the statutory reference in question – an equivalent oversight mechanism. […] 269

c) Finally, there are no adequate statutory safeguards to ensure that measures taken pursuant to § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act do not interfere with the core of private life, which enjoys absolute protection. 270

aa) Covert surveillance measures by the state must respect an inviolable core of private life protected under Art. 1(1) of the Basic Law (cf. BVerfGE 6, 32 <41>; 27, 1 <6>; 32, 373 <378 and 379>; 34, 238 <245; 80, 367 <373>; 109, 279 <313>; 113, 348 <390>). Even overriding public interests cannot justify an interference with this core (cf. BVerfGE 34, 238 <245>; 109, 279 <313>). The development of one's personality within the core of private life encompasses the possibility of expressing internal processes such as emotions and feelings, as well as reflections, views and experiences of a highly personal nature, without fear of surveillance by state authorities (cf. BVerfGE 109, 279 <314>). 271

In the context of covert access to information technology systems, there is a risk that the state collects personal data that can be attributed to the core of private life. This is the case, for instance, where the person concerned uses the system to create and store files with highly personal contents, such as diary-like notes, or private video or sound files. Such files may enjoy absolute protection, as may, *inter alia,* written accounts of highly personal experiences (cf. in this regard BVerfGE 80, 367 <373 *et seq.*>; 109, 279 <319>). Furthermore, if the system also serves telecommunications purposes, it might be used to transmit contents which may belong to the core of private life, too. This applies not only to voice telephony, but also to remote communications for instance via email or other Internet communication services (cf. BVerfGE 113, 348 <390>). […] 272

bb) In the event of covert access to information technology systems, special statutory safeguards are required that protect the core of private life of the affected person. 273

Citizens increasingly use complex information technology systems for managing personal matters and for telecommunications, including with persons they are close to. These systems provide them with opportunities for development in the highly personal domain. Compared to other surveillance measures – such as the use of GPS as a technical surveillance tool (cf. in this regard BVerfGE 112, 304 <318>) –, an investigation measure accessing an information technology system, which can be used to collect comprehensive data from the target system, thus gives rise to an increased risk of highly personal data being collected. 274

Because the accessing is carried out covertly, affected persons have no possibility to take steps for ensuring themselves, before or during the investigation measure, that the investigating authority respects the core of their private life. This complete loss of control must be countered by special provisions that afford protection by means of suitable procedural safeguards against the risk of violations of the core of private life. 275

cc) The constitutional requirements regarding the specific design of the framework ensuring protection of the core may differ depending on the method of data collection and the nature of the information obtained by it. 276

A statutory provision authorising a surveillance measure that might affect the core of private life must ensure, to the greatest extent possible, that no data relating to the core of private life is collected. If it is virtually unavoidable that information will be obtained before its link to the core can be determined – as is the case with covert accessing of information technology systems –, sufficient protection must be ensured at the stage of analysis. In particular, where data relating to the core was found and collected it must be deleted without undue delay and any further use must be ruled out (cf. BVerfGE 109, 279 <318>; 113, 348 <391 and 392>). 277

(1) In the context of covert access to an information technology system, data collection will be automated for technical reasons, at least in the vast majority of cases. In comparison with data collection carried out manually, this automated process makes it more difficult to distinguish at the stage of collection between data relating to the core and data not relating to the core. […] 278

Even if data is directly accessed manually without relying on prior technical recordings, for instance listening in on voice telephony via the Internet, protection of the core encounters practical difficulties even at the stage of data collection. Typically, when such a surveillance measure is carried out, it cannot be predicted with certainty what the contents of the collected data will be (cf. regarding telecommunications surveillance BVerfGE 113, 348 <392>). It may also be difficult to analyse the contents of the data while the collection process is ongoing. This applies for instance to text files or conversations in foreign languages. In this respect, it is not always possible to assess before or during data collection whether the communications under surveillance relate to the core of private life. However, if there is a risk that the data collection might violate the core of private life, this does not mean that constitutional law pre- 279

cludes the accessing of such information from the outset in these cases, given that the accessing of information technology systems is based on factual indications of a specific danger to an exceptionally significant legal interest.

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

(a) The statutory provision must ensure that the collection of data relating to the core is avoided from the outset as far as this is possible in terms of information technology and investigation technique (cf. regarding telecommunications surveillance BVerfGE 113, 348 <391 and 392>; regarding acoustic surveillance of private homes BVerfGE 109, 279 <318, 324>). In particular, safeguards made available by information technology must be used. If there are specific indications suggesting that a certain data collection measure will affect the core of private life in the individual case, it must in principle not be used. The situation is different if, for instance, specific indications suggest that core-related communication contents are deliberately linked to contents targeted by the investigation in order to evade surveillance. 281

(b) In many cases, the extent to which collected data relates to the core of private life cannot be determined before or during collection. The legislator must provide for suitable procedural safeguards to ensure that, where data relating to the core of private life has been collected, the severity of the violation of the core and its impact on the personality and development of the person concerned be kept to a minimum. 282

In this respect, it is crucial that the collected data be examined as to whether it contains information relating to the core of private life. Suitable procedures must be put in place that sufficiently protect the interests of the affected persons. If the examination reveals that data relating to the core was collected, it must be deleted without undue delay. Any sharing or use of this data must be ruled out (cf. BVerfGE 109, 279 <324>; 113, 348 <392>). 283

dd) The challenged Act lacks necessary provisions protecting the core. Even if the reference to the Article 10 Act in § 5(2) no. 11 second sentence of the NRW Constitution Protection Act were taken into account despite its shortcomings in terms of legal specificity, this would not merit a different conclusion, given that the Article 10 Act equally lacks safeguards protecting the core of private life. 284

[…] 285

d) The violation of the general right of personality in its manifestation as protection of the confidentiality and integrity of information technology systems (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law) renders § 5(2) no. 11 first sentence, second alternative of the NRW Constitution Protection Act void. 286

e) […] 287

II.

The legislative authorisation of covert Internet surveillance pursuant to § 5(2) no. 11 first sentence, first alternative of the NRW Constitution Protection Act violates the privacy of telecommunications under Art. 10(1) of the Basic Law. In certain cases, measures taken pursuant to this provision constitute interferences with this fundamental right that are not justified under constitutional law (see 1 below). Art. 19(1) second sentence of the Basic Law is also violated (see 2 below). Given that the provision is unconstitutional, it is declared void (see 3 below). Nevertheless, the *Land* Office for the Protection of the Constitution may in principle carry out Internet surveillance measures to the extent that these do not amount to interferences with fundamental rights (see 4 below). 288

1. The covert Internet surveillance provided for in § 5(2) no. 11 first sentence, first alternative of the NRW Constitution Protection Act covers measures carried out by the Office for the Protection of the Constitution to obtain knowledge of the contents of Internet communication via the normal technical means provided for this purpose, for instance by accessing a website on the World Wide Web using a web browser (see A I 1 a above). In certain cases, this may interfere with the privacy of telecommunications. The challenged provision does not justify such an interference under constitutional law. 289

a) The scope of protection of Art. 10(1) of the Basic Law covers ongoing telecommunications conducted via an information technology system that is connected to the Internet (see I 1 c aa (1) above). However, this fundamental right only protects individuals to the extent that they have the legitimate expectation that third parties cannot obtain knowledge of the telecommunications in which they are involved. By contrast, this fundamental rights protection does not extend to the legitimate expectations that communication partners have towards each other. […] Therefore, the fact that the state obtains knowledge of telecommunication contents must only be measured against the privacy of telecommunications if a state authority monitors a telecommunication relationship from the outside without being involved as a communicating party. […] 290

[…] 291

Covert Internet surveillance thus interferes with Art. 10(1) of the Basic Law if the Office for the Protection of the Constitution monitors secure communication contents by using access keys obtained without the consent or against the will of the communicating parties. This is the case, for instance, if a password obtained by way of keylogging is used in order to gain access to an email inbox or a private chatroom. 292

By contrast, there is no interference with Art. 10(1) of the Basic Law if for instance a participant in a private chatroom has voluntarily provided a person acting on behalf of the Office for the Protection of the Constitution with their access information, which the authority then uses. An interference with telecommunications privacy can certain- 293

ly be ruled out where the authority collects generally accessible contents, for instance by viewing open discussion forums or websites that are not password protected.

b) The interferences with Art. 10(1) of the Basic Law arising under § 5(2) no. 11 first sentence, first alternative of the NRW Constitution Protection Act are not justified under constitutional law. The challenged provision does not meet the constitutional requirements regarding authorisations for such interferences. 294

aa) § 5(2) no. 11 first sentence, first alternative of the NRW Constitution Protection Act does not satisfy the requirement of legal clarity and specificity given that the second sentence of this provision is too vague, failing to set out the prerequisites for interference in a sufficiently precise manner (see C I 2 a, bb above). 295

bb) Furthermore, to the extent that it is measured against Art. 10(1) of the Basic Law, the challenged provision does not satisfy the requirement of proportionality in the strict sense. 296

The interference with telecommunications privacy is serious. Based on the challenged provision, the Office for the Protection of the Constitution could access communication contents which may be sensitive, and which may provide insights into the personal matters and habits of the persons concerned. This holds true not only for the persons who prompted a surveillance measure; the interference may also indiscriminately affect other persons if the information obtained concerns not only persons targeted by the measure but also their communication partners. The covert nature of the accessing increases the severity of the interference. Additionally, given the broad wording of the prerequisites for interference in § 7(1) no. 1 in conjunction with § 3(1) of the NRW Constitution Protection Act, surveillance may also be directed against persons who did not prompt the interference. 297

Even when taking into account the significant weight attached to the pursued aim of protecting the constitutional order, an interference with fundamental rights of such severity in principle requires at least that the statutory basis set a qualified and substantive threshold for interference (cf. regarding criminal investigations BVerfGE 107, 299 <321>). With such a threshold lacking here, § 7(1) no. 1 in conjunction with § 3(1) of the NRW Constitution Protection Act authorises, on a large scale, purely precautionary intelligence service action before specific dangers actually materialise, but fails to take into account the weight of the legal interests, including of third parties, that are potentially violated as a result. Such a far-reaching legislative authorisation of fundamental rights interferences is not compatible with the principle of proportionality. 298

cc) With regard to interferences arising under § 5(2) no. 11 first sentence, first alternative of the NRW Constitution Protection Act, the statutory framework does not contain any safeguards protecting the core of private life. Yet such safeguards are necessary where state authorities are authorised to collect telecommunication contents in a manner that interferes with Art. 10(1) of the Basic Law (cf. BVerfGE 113, 348 299

<390 *et seq.*>).

2. Finally, to the extent that § 5(2) no. 11 first sentence, first alternative of the NRW Constitution Protection Act authorises interferences with Art. 10(1) of the Basic Law, the provision does not satisfy the requirement that the affected fundamental right be expressly specified (*Zitiergebot*) in accordance with Article 19(1) second sentence of the Basic Law. 300

[…] 301-302

3. Given that § 5(2) no. 11 first sentence, first alternative of the NRW Constitution Protection Act violates Art. 10(1) and Art. 19(1) second sentence of the Basic Law, the provision is void. 303

4. However, insofar as Internet surveillance measures do not interfere with fundamental rights, the voidness of the legislative authorisation does not generally bar the authority from taking such measures. 304

Covert surveillance that does not amount to an interference with Art. 10(1) of the Basic Law does not necessarily constitute an interference with the general right of personality guaranteed by Art. 2(1) in conjunction with Art. 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 the Internet surveillance measures pursuant to § 5(2) no. 11 first sentence, first alternative of the NRW Constitution Protection Act, given that these measures are limited to collecting data intended by the relevant system's owner – for instance the operator of a web server – for Internet communication purposes using the normal technical means provided in this regard. For these data collection purposes, the persons concerned themselves have allowed technical access to their systems. Therefore, they cannot legitimately expect that no such measures are taken. 306

b) As a general rule, there is also no interference with Art. 2(1) in conjunction with Art. 1(1) of the Basic Law in its manifestation as a right to informational self-determination. 307

aa) The state is not generally barred from obtaining publicly accessible information. This also applies if this possibility is used to collect personal information in the individual case […]. Therefore, it does not amount to an interference with the general right of personality if a state authority collects communication contents that are available on the Internet and addressed to the general public or to a group of persons that is not further defined. This is the case, for instance, where authorities view a generally accessible website on the World Wide Web, subscribe to a mailing list that is open to everyone or monitor an open chatroom. 308

Yet an interference with the right to informational self-determination may arise if information obtained by viewing generally accessible web contents is deliberately compiled, stored and, as the case may be, analysed using further data, giving rise to a 309

special risk to the personality of the person concerned. Such measures require a statutory basis authorising this interference.

bb) It does not constitute an interference with the right to informational self-determination if a state authority merely uses a cover identity to build a communication relationship with a fundamental rights holder. However, it does constitute an interference if, in doing so, it exploits that person's legitimate expectations regarding the identity and motivation of their communication partner, for the purposes of collecting personal data which the state authority would not receive otherwise […]. 310

It follows that, as a rule, Internet surveillance as such will generally not amount to an interference with fundamental rights. To a large extent, the communication relationships facilitated by Internet communication services do not merit legitimate expectations regarding the identity and authenticity of one's communication partners since these cannot be verified. This applies even if certain persons – for instance in the context of a discussion forum – participate in communication over a longer time period and thus form a kind of 'online community'. Even in this type of communication relationships, all participants are aware of the fact that they do not know the identity of their communication partners, or are in any case unable to verify the information those partners provide about themselves. Their expectation that they are not communicating with a state authority does thus not merit protection. 311

III.

[…] 312

IV.

§ 5a(1) of the NRW Constitution Protection Act is compatible with the Basic Law insofar as its scope of application was expanded to cover activities within the meaning of § 3(1) no. 1 of the NRW Constitution Protection Act. In particular, this provision does not violate Art. 2(1) in conjunction with Art. 1(1) of the Basic Law. 313

1. The collection of data on bank accounts and transactions provided for in § 5a(1) of the NRW Constitution Protection Act interferes with the general right of personality in its manifestation as a right to informational self-determination. 314

Such account information can be significant for protecting the personality of the persons concerned, and thus enjoy fundamental rights protection. […] 315

[…] 316

2. The interferences with fundamental rights authorised by § 5a(1) of the NRW Constitution Protection Act are, however, constitutionally justified with respect to investigating the activities specified in § 3(1) no. 1 of the NRW Constitution Protection Act. In particular, the challenged provision satisfies the principle of proportionality in this respect. 317

[…] 318-332

V.

[…] 333

Papier Hohmann-Dennhardt Hoffmann-Riem

Papier Hohmann-Dennhardt Hofmann-Riem

Bryde Gaier Eichberger

Schluckebier Kirchhof

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

Zitiervorschlag BVerfG, Beschluss 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