Headnotes

to the Order of the First Senate of 4 April 2006

1 BvR 518/02

1. **The type of electronic profiling and searches provided for in § 31 of the 1990 North Rhine-Westphalia Police Act as a preventive police measure is only compatible with the fundamental right to informational self-determination (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law) if there is a specific danger to high-ranking legal interests such as the existence or security of the Federation or a *Land* or life, limb or liberty of the person. Such electronic profiling is impermissible if it serves as a purely precautionary measure before a danger to public security arises.**

2. **Neither a general threat situation, such as the persistent threat of terrorism since the 9/11 attacks, nor foreign policy tensions constitute sufficient grounds for ordering electronic profiling. Rather, such measures require further facts indicating the existence of a specific danger, such as the danger of a terrorist attack being prepared or carried out.**

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 518/02 -

IN THE NAME OF THE PEOPLE

In the proceedings
on the constitutional complaint of

Mr A...

– authorised representative: …

against a) the Order of the Düsseldorf Higher Regional Court of 8 February 2002 - 3 Wx 356/01 -,

b) the Order of the Düsseldorf Regional Court of 29 October 2001 - 25 T 873/01 -,

c) the Order of the Düsseldorf Local Court of 2 October 2001 - 151 Gs 4092/01 -

the Federal Constitutional Court – First Senate –

with the participation of Justices

President Papier,

Haas,

Hömig,

Steiner,

Hohmann-Dennhardt,

Hoffmann-Riem,

Bryde,

Gaier

held on 4 April 2006:

The Order of the Düsseldorf Higher Regional Court of 8 February 2002 - 3 Wx 356/01 -, the Order of the Düsseldorf Regional Court of 29 October 2001 - 25 T 873/01 - and the Order of the Düsseldorf Local Court of 2 October 2001 - 151 Gs 4092/01 - violate the complainant's fundamental right under Article 2(1) in conjunction with Article 1(1) of the Basic Law. The orders of the Higher Regional Court and the Regional Court are reversed. The matter is remanded to the Regional Court.

[…]

REASONS:

A.

The constitutional complaint challenges judicial decisions on electronic profiling and searches (*Rasterfahndung*) as a preventive police measure. 1

I.

1. Electronic profiling is a special investigation technique that uses electronic data processing for conducting police searches. The police authorities request that other public or private bodies share personal data held by them, which is cross-checked against other data in an automated procedure (profiling). This data cross-checking serves to identify persons that match certain criteria, which must be defined in advance and be considered significant for furthering the investigations. 2

In Germany, electronic profiling was first conceived in the 1970s in connection with the fight against terrorism. […] 3

[…] 4-6

2. Following the 9/11 terrorist attacks, information emerged that some of the perpetrators had resided in Germany. The *Land* police authorities, together with the Federal Criminal Police Office (*Bundeskriminalamt*), carried out coordinated nationwide electronic profiling measures in search of Islamist terrorists […]. In particular, these measures were aimed at detecting so-called sleeper terrorists […]. 7

[…] According to information provided by the Federal Data Protection Officer, the [competent] coordination committee developed a set of profiling criteria for identifying potential Islamist terrorists in Germany. Next, the *Land* Criminal Police Offices (*Landeskriminalämter*) obtained data from universities, residents' registration offices (*Einwohnermeldeämter*) and the Central Register of Foreigners (*Ausländerzentralregister*), which they then filtered based on the following criteria: male, 18 to 40 years of age, student or former student, Muslim faith, born in a country with a majority Muslim population (as specified on a list of relevant countries) or national of such a country […]. 8

The data records which yielded positive matches in this cross-checking were transmitted to the Federal Criminal Police Office, which entered the data into the joint national database on sleeper terrorists. According to the Federal Criminal Police Office, it received more than 31,988 data records from the *Länder*. The records were subsequently cross-checked against other data records obtained by the Federal Criminal Police Office. The data used for cross-checking […] included, for example, records kept on holders of pilot licences and records kept on persons requiring special security clearance pursuant to § 12b of the Atomic Energy Act. […] The matches from the cross-checking were compiled in a database which was made available to the *Land* Criminal Police Offices. […] 9

To date, not a single case has emerged in which these electronic profiling measures led to the identification of sleeper terrorists, let alone to charges being brought against one of the profiled persons based on evidence thus obtained – for instance on the grounds that they were members or supporters of a terrorist organisation (cf. §§ 129a, 129b of the Criminal Code). 10

II.

1. The *Land* North Rhine-Westphalia participated in the coordinated nationwide electronic profiling measures. 11

a) By the order challenged in the present constitutional complaint proceedings, the Local Court authorised electronic profiling measures on 2 October 2001 at the request of the Düsseldorf police. The court order compelled all residents' registration offices of the *Land* North Rhine-Westphalia, the Central Register of Foreigners based in Cologne, and all universities, higher education institutions and universities of applied sciences in North Rhine-Westphalia to share [certain personal] data on men born between 1 October 1960 and 1 October 1983. […] 12

[…] 13

b) The court order was based on § 31 of the NRW Police Act in the version published on 24 February 1990 (GVBl p. 70). […] 14

[…] 15-20

The provision was amended in 2003. In the version published on 25 July 2003 (GVBl p. 441), § 31(1) of the NRW Police Act no longer requires the existence of a present danger (*gegenwärtige Gefahr*). […] 21

[…] 22-26

2. Based on the challenged court order, electronic profiling was further carried out in North Rhine-Westphalia as follows: 27

The bodies addressed by the order first transferred approximately 5.2 million data records compiled according to the "criteria for selecting persons of interest". […] 28

In an automated procedure, these data records were then cross-checked against the further profiling criteria that had been agreed as part of the nationwide coordination of the measure. According to information by the Ministry of Justice of the *Land* North Rhine-Westphalia, this resulted in 11,004 data records with positive matches. According to the Officer for Data Protection and Freedom of Information for the *Land* North Rhine-Westphalia, the other data records (5,222,717) were deleted by 10 December 2001. The data storage devices provided by the transferring bodies were destroyed. 29

[…] 30-33

III.

1. The complainant, who was born in 1978, is a Moroccan national of Muslim faith. At the time the challenged order was issued, he was a student at Duisburg University. He filed a complaint against the order of the Local Court. […] 34

In an order that is also challenged in the present proceedings, the Regional Court rejected the complaint as unfounded. […] 35

[…] 36-37

2. The complainant filed a further complaint against the Regional Court's order, which was rejected by the Higher Regional Court in an order that is also challenged here. […] 38

[…] 39-49

IV.

1. The complainant claims that the challenged court decisions violate his fundamental right to informational self-determination under Art. 2(1) in conjunction with Art. 1(1) of the Basic Law. 50

[…] 51-56

V.

Statements on the constitutional complaint were submitted by the Ministry of Justice of the *Land* North Rhine-Westphalia, the Officer for Data Protection and Freedom of Information of the *Land* North Rhine-Westphalia, the Federal Criminal Police Office and the Federal Data Protection Officer. 57

[…] 58-64

B.

The constitutional complaint is admissible and well-founded. 65

The challenged decisions violate the complainant's fundamental right to informational self-determination under Art. 2(1) in conjunction with Art. 1(1) of the Basic Law. While the statutory provision on which the interferences are based is constitutional, the courts have interpreted the provision in a manner that is incompatible with the aforementioned fundamental right; even the legislator could not have enacted statutory provisions with the contents of the courts' interpretation without violating this fundamental right. The application of the provision in the case at hand is based on this [unconstitutional] interpretation. 66

I.

The court order authorising electronic profiling is based on § 31(1) of the 1990 NRW Police Act; this provision is formally and substantively compatible with the Constitution. 67

1. § 31(1) of the 1990 NRW Police Act authorises interferences with the fundamental right to informational self-determination guaranteed by Art. 2(1) in conjunction with Art. 1(1) of the Basic Law. 68

a) Based on the notion of self-determination, this right confers upon the individual the authority to, in principle, decide themselves whether and to what extent to disclose aspects of their personal life (cf. BVerfGE 65, 1 <43>; 78, 77 <84>; 84, 192 <194>; 96, 171 <181>; 103, 21 <32 and 33>; 113, 29 <46>). It affords fundamental rights holders protection against the unlimited collection, storage, use or sharing of personal data that is individualised or that can otherwise be attributed to them as individual persons (cf. BVerfGE 65, 1 <43>; 67, 100 <143>; 84, 239 <279>; 103, 21 <33>; BVerfGE 115, 166 <188>). It is a prerequisite for individual self-determination – especially in light of modern information technology – that the individual be afforded the freedom to decide whether to take or refrain from certain actions, including the possibility to actually conduct themselves in accordance with this decision. If individuals cannot, with sufficient certainty, determine what kind of personal information is known to certain parts of their social environment, and if it is difficult to ascertain what kind of information potential communication partners are privy to, this could greatly impede their freedom to make self-determined plans or decisions (cf. BVerfGE 65, 1 <42 and 43>). 69

Monitoring or surveillance measures by the police can affect the scope of protection of this fundamental right and amount to interferences (cf. BVerfGE 110, 33 <56>). This holds true in particular where personal data is collected and stored for the purposes of electronic data processing. As a consequence, this data can be retrieved at any time within seconds, without distance being an issue. In addition, the personal data in question can be compared with data collected from other sources, especially by creating integrated information systems, allowing for numerous possibilities of using and linking the data (cf. BVerfGE 65, 1 <42>). The increased risk associated with such technical possibilities in the context of modern data processing is reflected in 70

the level of fundamental rights protection afforded in this respect (cf. BVerfGE 65, 1 <42>; 113, 29 <45 and 46>).

b) The authorisation of measures under § 31 of the 1990 NRW Police Act affects the scope of protection of the right to informational self-determination. 71

The statutory powers concern different types of information that vary in their relevance to the right of personality. There is no need to determine whether the right to informational self-determination affords protection against the collection of each individual data item covered by the measure, since the knowledge of each data item in connection with other data allows for distinct insights into one's personal domain. The combination of the data expressly listed in § 31(2) of the 1990 NRW Police Act – name, address, date and place of birth – with other data such as, in the present case, nationality, religion or field of studies can, and is intended to, provide information on certain behaviours that may be considered suspicious; specifically, this refers to "characteristics increasing potential danger associated with these persons" – as is now explicitly stated in the amended § 31(1) of the 2003 NRW Police Act. The fundamental right to informational self-determination affords protection against the collection and processing of data carried out to this end. 72

c) § 31(1) of the 1990 NRW Police Act authorises interferences with the fundamental right to informational self-determination of the persons whose data is shared [for the purposes of electronic profiling]. 73

aa) The court order for the sharing of the requested data constitutes an interference, given that it provides the basis for recording and storing the data and for cross-checking it against other data. The resulting effects on the right to personal self-determination of affected persons show that the order amounts to an interference. It makes the data available to the authorities and is the basis for the subsequent cross-checking with search terms. This qualifies as an interference, unless data is recorded incidentally for purely technical reasons and then deleted immediately and anonymously, without leaving traces and without any interest on the part of the authorities in obtaining knowledge of the data (cf. BVerfGE 100, 313 <366>; 107, 299 <328>). […] 74

Electronic profiling pursuant to § 31(1) of the 1990 NRW Police Act certainly amounts to an interference with respect to persons whose data is subject to further measures, in particular further cross-checking, after the initial cross-checking has been concluded. The order to share data impairs these persons' right to informational self-determination [...] and makes them a potential target of state surveillance measures. 75

In the case at hand, the sharing of data must be considered an interference with fundamental rights regarding the approximately 11,000 persons whose data records were initially selected for further processing measures after they were singled out from the records shared by the *Land* authorities since they matched the criteria agreed in the nationwide coordination of the measure. The records that yielded posi- 76

tive matches were forwarded to the Federal Criminal Police Office for further processing; they were entered into the national sleeper database and cross-checked against further databases. […]

[…] 77

bb) The storage of the data – even if it is only temporary – by the receiving body, which retains it and makes it available for cross-checking, interferes with the right to informational self-determination of the persons whose data is subject to further measures after the initial cross-checking (cf. BVerfGE 100, 313 <366>). 78

cc) With respect to these persons, even the cross-checking of the data itself amounts to an interference as it determines the selection of data for further analysis (cf. BVerfGE 100, 313 <366>). 79

2. The authorisation to interfere with fundamental rights laid down in § 31(1) of the 1990 NRW Police Act satisfies the constitutional requirements. 80

a) The fundamental right to informational self-determination is not guaranteed without limitation. Rather, the individual must accept that this right is subject to restrictions serving overriding public interests (cf. BVerfGE 65, 1 <43 and 44>). However, such restrictions require a statutory basis that must be constitutional, satisfying in particular the requirements of proportionality and legal clarity (cf. BVerfGE 65, 1 <44>). 81

b) § 31(1) of the 1990 NRW Police Act, which restricts the aforementioned fundamental right, satisfies the principle of proportionality. This principle requires that the state, in interfering with fundamental rights, pursue a legitimate purpose by suitable, necessary and appropriate means (cf. BVerfGE 109, 279 <335 *et seq*.>). 82

aa) The provision serves the legitimate purpose of averting danger to the existence or security of the Federation or a *Land*, or to life, limb or liberty of the person. 83

bb) Electronic profiling is also a suitable means for achieving this purpose. 84

A law is suitable for achieving its purpose if it is conducive to the outcome sought (cf. BVerfGE 67, 157 <173, 175>; 90, 145 <172>; 100, 313 <373>; 109, 279 <336>). This is the case here. The suitability of the statutory provision is not called into question merely because the method of data collection indiscriminately affects a large number of persons yet only yields useful intelligence in comparatively few cases (cf. BVerfGE 100, 313 <373>). 85

cc) The interference is also necessary for achieving the legislative purpose. There are no less restrictive means that would be equally effective in achieving the purpose pursued. 86

dd) The statutory authorisation respects the limits of proportionality in its strict sense. 87

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 (established case-law; cf. BVerfGE 90, 145 <173>; 92, 277 <327>; 109, 279 <349 *et seq*.>). Based on this standard, the review of proportionality may lead to the conclusion that even though a measure protecting legal interests is suitable and necessary as such, it is nevertheless impermissible because the resulting interferences with fundamental rights would outweigh the gain in protection of legal interests, rendering the use of the measure in question inappropriate (cf. BVerfGE 90, 145 <173>). 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 when the suspicion or danger prompting the interference reaches a certain threshold. 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*.> […]). 88

In the context of electronic profiling, this requires that the legislator make the measures resulting in interferences with fundamental rights contingent upon the existence of a specific danger (*konkrete Gefahr*) to the legal interests under threat. § 31(1) of the 1990 NRW Police Act meets this standard. 89

(1) The interference authorised by § 31 of the 1990 NRW Police Act serves to protect high-ranking constitutional interests. 90

The existence and the security of the Federation and of the *Länder*, as well as life, limb and liberty of the person, which the provision aims to protect against dangers, are legal interests of significant constitutional weight. 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 – while respecting the dignity and the intrinsic value of the individual – rank equally with other constitutional values that are accorded high standing (cf. BVerfGE 49, 24 <56 and 57>). 91

[…] 92

(2) In order to protect these legal interests, § 31 of the 1990 NRW Police Act authorises particularly weighty interferences with the right to informational self-determination. 93

(a) In the legal assessment of the type of interferences covered by the statutory authorisation, it is significant *inter alia* how many holders of fundamental rights are affected by impairments, how intense these impairments are, and on what basis they occur, in particular whether the affected persons have prompted them (cf. BVerfGE 100, 313 <376>*;* 107, 299 <318 *et seq*.>; 109, 279 <353>). Thus, relevant criteria include the design of the statutory thresholds for carrying out the measures constituting 94

interferences, the number of persons affected and also the severity of the individual impairments (cf. BVerfGE 100, 313 <376>). The weight of individual impairments depends on whether the persons concerned remain anonymous, what personal information is recorded, and what disadvantages the holders of fundamental rights might face or have reason to fear on account of the measures (cf. BVerfGE 100, 313 <376>; 109, 279 <353>).

The Federal Constitutional Court has so far primarily developed criteria for assessing the severity of interferences with information-related fundamental rights in decisions concerning the privacy of telecommunications under Art. 10(1) of the Basic Law and the fundamental right to the inviolability of the home under Art. 13(1) of the Basic Law. As these are specific manifestations of the fundamental right to informational self-determination (cf. BVerfGE 51, 97 <105>; 100, 313 <358>; 109, 279 <325 and 326>), the standards developed in this regard also apply to the more general fundamental right at issue here, unless they are informed by considerations that are particular to the specific guarantees [under Art. 10 and Art. 13 of the Basic Law]. 95

(b) It is true that electronic profiling concerns information that in itself is typically less closely related to one's personality than is the case for information resulting in interferences with the fundamental rights under Art. 10(1) and Art. 13(1) of the Basic Law. Nevertheless, the interferences resulting from electronic profiling are also of considerable weight in view of the general fundamental right to informational self-determination, given the broad substantive scope of the authorisation and the possibilities it creates for the linking of data. 96

(aa) The weight of an interference with the right to informational self-determination depends, *inter alia*, on what information is subject to the interference, in particular how closely related the information is to one's personality, both in itself and when linked to other information, and on the way it is obtained (cf. BVerfGE 100, 313 <376>; 107, 299 <319 and 320>; 109, 279 <353>). 97

Accordingly, the interference is particularly intrusive where it concerns information obtained in violation of expectations of confidentiality, especially in matters that are afforded special fundamental rights protection, as is the case regarding interferences with the fundamental right to the inviolability of the home under Art. 13 of the Basic Law or the privacy of telecommunications under Art. 10 of the Basic Law (cf. BVerfGE 109, 279 <313 and 314, 325, 327 and 328>; 113, 348 <364 and 365, 383, 391>). 98

All information covered by electronic profiling relates to individuals and provides insights regarding their personality, given that the information is linked to other data. Information that is particularly closely related to one's personality includes, most notably, information pertaining to matters protected by further constitutional guarantees, such as Art. 3(3) of the Basic Law or Art. 140 of the Basic Law in conjunction with Art. 136(3) of the Weimar Constitution. At the level of statutory law, this is reflected in the recognition of "special categories of personal data" in § 3(9) of the Federal Data Protection Act. These categories include information on racial and ethnic origin, polit- 99

ical opinions, religious or philosophical beliefs, trade union membership and data concerning one's health or sex life.

(bb) The interference with fundamental rights authorised in the statutory basis for electronic profiling generally has considerable weight in view of the contents of both the data shared for this purpose and the data used for cross-checking. The same applies to further information that can be obtained from linking and cross-checking the different data records. 100

The data shared for the purposes of electronic profiling as such can already be closely related to an individual's personality. Based on the provision's legislative history, electronic profiling primarily focuses on the specifically listed identifying data, i.e. name, address, date and place of birth. Yet the statutory authorisation is not limited to this data. Rather, it also allows "any other type of data, as necessary in the individual case" to be included in the measure (§ 31(2) first sentence, first half-sentence of the 1990 NRW Police Act). The only data that may not be requested is personal data protected by professional confidentiality or special rules of official secrecy (§ 31(2) first sentence, second half-sentence of the 1990 NRW Police Act). Other than that, the provision does not further restrict the type and contents of the data used in electronic profiling. Accordingly, data requests can be extended to include further information on religion, nationality, civil status and field of studies – which occurred in the case at hand. The statutory authorisation thus also covers personal data that individuals may very much want to keep private and that they expect to be treated confidentially, such as one's religious beliefs. This may also be true with regard to the "other data records" against which the shared data is cross-checked. In addition, the compiling and linking of the shared data sets and other data sets, and the mutual cross-checking of the data, may yield a wide variety of new information. The type and contents of this new information may have a particularly close link to one's personality. 101

(c) When an authorisation to share data extends to almost all personal data available at any public or non-public body, like the authorisation under § 31(1) of the 1990 NRW Police Act, it creates the basis for particularly intrusive interferences due to the variety and scope of the data that may be subject to the authorised measures. 102

Apart from the general requirement of proportionality (cf. § 2 of the 1990 NRW Police Act), the NRW Police Act does not provide for any limitation regarding the scope of data that may be requested for the purposes of electronic profiling. There is no such limitation, not even an indirect one, neither regarding the type of data requested nor regarding targeted persons, given that any public body and any "body outside the public sector" can be requested to share data according to the wording of § 31(1) of the 1990 NRW Police Act. The provision covers all bodies controlling personal data, with the exception of matters for which sector-specific rules set out definitive prohibitions of data sharing. […] 103

The authorisation thus makes it possible for one body, where that body considers it necessary, to centrally compile and cross-check all data – concerning any person 104

and stored at any public or private body –, subject to the restriction laid down in § 31(2) of the 1990 NRW Police Act and the general limits set by the principle of proportionality. In doing so, it uses the unique possibilities created by information technologies with regard to the processing and linking of data. Therefore, data that by itself appears insignificant may gain new relevance (cf. BVerfGE 65, 1 <45>).

Consequently, there is a risk that the strict prohibition of collecting data for retention, other than for statistical purposes (cf. BVerfGE 65, 1 <47>), is circumvented. [...] 105

Moreover, given the amount and variety of personal data available today on almost any person – when looking at all the data held by public and private bodies combined – the authorisation to access data under § 31 of the 1990 NRW Police Act comes at least close to allowing the linking of data from different data collections to create partial or almost complete personality profiles – which would be impermissible under constitutional law (cf. BVerfGE 65, 1 <42>). In particular, the statutory authorisation also applies to all data records held by private bodies (“bodies outside the public sector”) […]. To satisfy constitutional law, the statutory authorisation to access data under § 31 of the 1990 NRW Police Act must be interpreted to the effect that it does not allow for a comprehensive registration and cataloguing of one’s personality by means of compiling personality profiles of the citizens concerned on the basis of their biographical and personal data – this would be impermissible even if it were done anonymously for statistical surveys (cf. BVerfGE 65, 1 <53>). Nonetheless, the collection and linking of certain data authorised in that provision might come close to the creation of personality profiles, which is why the resulting interference with fundamental rights must be regarded as particularly intrusive. 106

(d) The severity of the interference is furthermore determined by other possible consequences resulting from electronic profiling. 107

The weight of information-related interferences with fundamental rights *inter alia* depends on the disadvantages that affected persons might face or have reason to fear on account of the interferences (cf. BVerfGE 100, 313 <376>; 107, 299 <320>). The sharing and use of data may expose affected persons to an increased risk of becoming the target of investigation measures by the state, beyond the general risk of being falsely suspected of wrongdoing (cf. BVerfGE 107, 299 <321>). In addition, information-related investigation measures may stigmatise affected persons in the event that these measures become publicly known. This may indirectly increase these persons’ risk of being discriminated against in their everyday or professional life. 108

Both these concerns apply to the interferences with fundamental rights linked to electronic profiling. 109

(aa) The fundamental rights holders affected by interferences resulting from electronic profiling face an increased risk of becoming the target of further investigation measures carried out by the authorities. […] 110

(bb) Furthermore, electronic profiling based on certain criteria that is carried out by 111

the police may stigmatise persons who meet these criteria if the measures become publicly known. […] The more closely the attributes determining who is targeted by state measures resemble the grounds listed in Art. 3(3) of the Basic Law, the more strictly the authorities are bound by the right to equality under constitutional law (established case-law; cf., e.g., BVerfGE 92, 26 <51>) and the higher the severity of an interference with fundamental rights linked to unequal treatment – in this case with the fundamental right to informational self-determination –, even if the measure as such does not amount to discrimination based on the grounds of Art. 3(3) of the Basic Law.

For instance, for determining the severity of the interference resulting from the electronic profiling measures carried out after 9/11, it is significant that they are directed against foreigners of a certain origin and Muslim faith. Such measures invariably entail the risk of perpetuating prejudice and stigmatising these communities in the public eye. […] This bears on the severity of the interferences under the statutory authorisation of § 31(1) of the 1990 NRW Police Act, which allows for electronic profiling measures that differentiate based on such criteria. 112

(e) The fact that the statutory provision only provides for individual notification of some but not all affected persons, and only upon completion of the electronic profiling measure, also bears on the severity of the interference. Covert measures by the state result in more intrusive interferences (cf. BVerfGE 107, 299 <321>; 115, 166 <194>). § 31(5) first sentence of the 1990 NRW Police Act only provides for individual notification of affected persons, once electronic profiling has been concluded, in cases where further measures are carried out against these persons, and only if it does not jeopardise the purpose of further data use. Pursuant to § 31(5) second sentence of the 1990 NRW Police Act, affected persons are not notified if, based on the facts [established during the measure], criminal investigations are launched against them. 113

It is true that the requirement of a judicial order under § 31(4) first sentence of the 1990 NRW Police Act mitigates the covert nature of the measure, provided that the order is made public – as was the case here […]. This allows persons potentially affected to realise that they are part of the group of persons targeted by electronic profiling. They may then seek legal protection – like the complainant in the case at hand. However, the law does not require publication of the order. If, unlike in this case, it is not made public, affected persons remain oblivious, unless they are individually notified. 114

(f) It is also significant that persons affected by electronic profiling do not always remain anonymous (cf. BVerfGE 100, 313 <381>; 107, 299 <320 and 321>). The anonymity is lifted at least regarding the persons whose data shows up as a match in the final results once the profiling as such has been concluded. The data of these persons is personalised precisely to make it possible to carry out further investigation measures against them. 115

(g) Finally, it is also significant that § 31(1) of the 1990 NRW Police Act provides for 116

interferences with fundamental rights that do not require any grounds for suspicion and indiscriminately affect a large number of persons.

(aa) Interferences with fundamental rights are generally particularly intrusive if they do not require any grounds for suspicion and indiscriminately affect a large number of persons, i.e. if the measure affects numerous persons who are neither connected to specific wrongdoing nor prompted the interference with their conduct (cf. BVerfGE 100, 313 <376, 392>; 107, 299 <320 and 321>; 109, 279 <353>; 113, 29 <53>; 113, 348 <383>). The less individuals prompted the state interference, the more severely their fundamental rights are affected. Such interferences may also create chilling effects, which may impair the exercise of fundamental rights (cf. BVerfGE 65, 1 <42>; 113, 29 <46>). A deterrent effect on the exercise of fundamental rights must be avoided, not only to protect the subjective rights of the individuals concerned. It would also affect the common good because self-determination is a fundamental prerequisite for the functioning of a free and democratic society which relies on the agency and participation of its citizens (cf. BVerfGE 113, 29 <46>). People might no longer act without worry or fear if the indiscriminate effect of investigation measures contributes to risks of abuse and a sense of being under surveillance (cf. BVerfGE 107, 299 <328>). 117

(bb) Electronic profiling pursuant to § 31(1) of the 1990 NRW Police Act constitutes an interference that does not require any grounds for suspicion. The provision confers powers to carry out interferences against persons who are not themselves linked to a danger to public security (*Nichtstörer*), as it does not require that the target of the measure constituting an interference be responsible for the danger in question. According to the 1990 version of the law, the measure can be extended to all persons who meet the selection criteria, without setting out any requirements as to the proximity of these persons to the danger or to persons of interest. […] 118

Particularly in cases where electronic profiling serves to uncover so-called sleeper terrorists, it constitutes an “interference for the purposes of identifying suspicious activities or persons of interest” (*Verdachts- oder Verdächtigungsgewinnungseingriff*) […]. Given the presumption that sleepers are characterised precisely by their completely conformist and thus inconspicuous behaviour, there are, by definition, no specific indications of behaviour that might point to them as persons responsible for potential dangers. Therefore, electronic profiling that aims to identify such persons requires that profiles of perpetrators be based on relatively unspecific assumptions and, accordingly, that unspecific search criteria be applied. As a consequence, and in a departure from traditional principles of police law governing public security, the search measures take place on grounds so precautionary in nature that a specific suspicion that someone poses a danger has not arisen yet. This differs fundamentally from a situation where the authorities search for a group of perpetrators who are in principle identifiable through specific behaviour that deviates from the norm. [...] 119

Compared to the circumstances typical of earlier electronic profiling measures, the fact that the measure at issue does not require any grounds for suspicion is further 120

aggravated as precisely the inconspicuousness and conformity of behaviour become a significant criterion in the search. This is obvious in the coordinated electronic profiling measures carried out across Germany in the present case. There were no specific indications to suggest even remotely that precisely the persons affected by the measure were so-called sleepers or were in contact with such sleepers; this is true for the approximately 5.2 million persons whose data was transferred to the Düsseldorf police and for the approximately 32,000 persons whose data was included in the nationwide database of sleepers according to information provided by the Federal Data Protection Officer. […]

(cc) Moreover, electronic profiling can have indiscriminate effects on an exceptionally large number of persons, as shown by the number of persons affected in the case at hand. 121

(α) As a search method, electronic profiling offers the advantages generally associated with automated, computer-based operations, i.e. the ability to process virtually unlimited and complex information at high speed. This leads to an unprecedented leap of effectiveness in relation to conventional investigation methods, where authorities operate by gradually gathering and connecting more and more relevant information […]. With regard to fundamental rights, this new quality of police investigation measures results in more intrusive interferences. 122

(β) To assess the appropriateness of such measures, not only the number of persons affected by electronic profiling in a manner that qualifies as an interference with their fundamental rights must be taken into account, but also the overall number of persons whose data is covered by the measure, due to the objective importance of the fundamental right to informational self-determination (cf. BVerfGE 107, 299 <328>). 123

If data is compiled according to relatively unspecific criteria, a very large number of persons may initially be affected by electronic profiling who, from an *ex ante* perspective, are neither suspicious nor linked to a danger. Even the group of persons that fit the search criteria used in an initial cross-checking may – as the present case shows – comprise a large number of persons that even from an *ex post* perspective are not linked to a danger, at least in the vast majority of cases. 124

(3) Given the high-ranking constitutional interests that § 31(1) of the 1990 NRW Police Act serves to protect, the interference resulting from electronic profiling is not disproportionate as such. Nevertheless, the measure constituting an interference is only appropriate if the legislator observes the requirements deriving from the rule of law by subjecting the measure to a threshold in the form of a sufficiently specific danger to the legal interests under threat. 125

(a) The state may, and must, effectively counteract terrorist threats with the necessary means permissible under the rule of law; these threats include, for instance, endeavours that aim to destroy the free democratic basic order and that use systematic 126

killing as a means to realise this aim (cf. BVerfGE 49, 24 <56>). Yet the Basic Law also requires that state action remain limited to the means permissible under the rule of law.

The Basic Law contains a mandate to avert impairments to the foundations of the free and democratic order, subject to the requirements deriving from the rule of law (cf. BVerfGE 111, 147 <158>; […]). The strength of the state under the rule of law is reflected precisely in its adherence to general principles, even in the face of its adversaries […]. 127

This also applies when the state pursues the fundamental aims of ensuring the security and protection of its people. The Constitution requires that the legislator strike an appropriate balance between freedom and security. This does not only preclude the state from seeking to attain absolute security, which in practice could hardly be achieved anyway, at least not without the sacrifice of abolishing freedom. Under the Basic Law, the aim of attaining the highest level of security possible under the given circumstances is subject to restrictions deriving from the rule of law, including the prohibition of inappropriate interferences with fundamental rights in their dimension as rights defending against state interference. 128

This prohibition also limits the state's duties of protection. Fundamental rights serve to protect the sphere of individual freedom against interference by public authorities; they are defensive rights of the citizen against the state (cf. BVerfGE 7, 198 <204 and 205>). Where fundamental rights function as objective principles, giving rise to duties of protection (cf. BVerfGE 96, 56 <64>), this function serves, in principle, to strengthen the normative force of fundamental rights; however, this function still remains rooted in the primary function of fundamental rights as defensive rights (cf. BVerfGE 50, 290 <337>). 129

When choosing the means for fulfilling a constitutional duty of protection, the state is thus limited to using means that are compatible with the Constitution (cf. BVerfGE 115, 118 <160>). Regardless of the weight attached to the constitutional interests the state is bound to protect, interferences with the absolutely protected right of the individual to respect for one's person (*Achtungsanspruch*) (cf. BVerfGE 109, 279 <313>) are always prohibited (cf. BVerfGE 115, 118 <152 *et seq*.>). Yet, even where a balancing of interests is required under the principle of proportionality in its strict sense, the duties of protection under the Basic Law must not be invoked so as to render meaningless the prohibition of inappropriate interferences with fundamental rights, with the effect that the principle of proportionality would no longer afford protection except in cases of unsuitable or unnecessary interferences. 130

(b) […] 131

(c) In the context of electronic profiling pursuant to § 31(1) of the 1990 NRW Police Act, the principle of proportionality does not give rise to an absolute prohibition of interferences with personality-related fundamental rights for investigative purposes. 132

However, the authorisation to carry out electronic profiling resembles measures interfering with the privacy of telecommunications for strategic surveillance purposes to the extent that the aforementioned authorisation also provides for interferences with fundamental rights that do not require any grounds for suspicion and indiscriminately affect a large number of persons. [...]

(d). The interferences with fundamental rights resulting from electronic profiling are of considerable weight, especially considering that the prerequisites for such interferences are not narrowly defined in the law. As a result, it is only permissible for the legislator to authorise electronic profiling for the protection of the high-ranking legal interests set out in § 31(1) of the 1990 NRW Police Act on condition that there is a specific danger to these interests. 133

When the legislator designs powers to carry out measures constituting interferences, it is not necessarily bound by the limits to interferences deriving from the traditional understanding of the term ‘danger’ in police law. However, where the severity of interference is as high as in the present case, the legislator may only set a lower threshold if particular proportionality requirements are observed. Yet these requirements are not met if the measure constituting an interference with fundamental rights does not require any grounds for suspicion, which is the case for electronic profiling. Therefore, under constitutional law, electronic profiling may only be carried out in cases of specific danger [as the relevant threshold]. 134

(aa) The Constitution does not generally prevent the legislator from further developing, in line with its prerogative, the traditional requirements deriving from the rule of law in the field of police law on the basis of new or evolving situations of danger and threat. The legislator may readjust the balance between freedom and security, yet it must not fundamentally shift the underlying weighing. 135

With respect to the principle of proportionality in the strict sense, the legislator must maintain a balance between the type and severity of the impairments of fundamental rights on the one hand and the statutory prerequisites for carrying out the measures constituting interferences on the other hand, such as the statutory threshold for interference, the required factual basis and the weight of the protected legal interests (cf. BVerfGE 100, 313 <392 *et seq*.>). The greater the weight of possible or actual impairments of legal interests and the lesser the weight of the interference with fundamental rights at issue, the more acceptable it becomes to lower the degree of probability required for establishing a violation (or risk thereof) of the respective legal interest, and the degree of certainty required for establishing the facts on which the suspicion is based (cf. BVerfGE 100, 313 <392>; 110, 33 <60>; 113, 348 <386>). However, the statutory requirements pertaining to the degree of probability and the factual basis of the prognosis must not be lowered arbitrarily; rather, they must be proportionate to the type and intensity of the resulting impairment of fundamental rights and to the prospects of success regarding the intended protection of legal interests. Even where the threats the interference aims to avert concern exceptionally 136

weighty legal interests, 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>). In particular, the Constitution does not allow interferences with fundamental rights that result from purely speculative investigations (cf. BVerfGE 112, 284 <297>; […]).

In accordance with the principle of proportionality, the legislator may only provide for particularly intrusive interferences with fundamental rights in the event that certain levels of suspicion or danger are met (cf. BVerfGE 100, 313 <383 and 384>; 109, 279 <350 *et seq*.>). […] The question whether an interference with fundamental rights for the purposes of averting potential future impairments of legal interests, as a purely precautionary measure before a specific danger arises, can be considered proportionate depends not only on its prospects of success (cf. on the requirement of sufficient prospects of success BVerfGE 42, 212 <220>; 96, 44 <51>; 115, 166 <198>); it also depends on the requirements laid down in the statutory provision governing the interference regarding the connection between the persons affected by the measure and the threat to the legal interest in question (cf. BVerfGE 100, 313 <395>; 107, 299 <322 and 323, 329>; 110, 33 <60 and 61>; 113, 348 <385 *et seq*., 389>). If the legislator authorises particularly serious interferences but fails to set restrictive requirements pertaining to the probability that the danger will materialise and to a sufficient connection between the affected persons and the threat the measure seeks to avert, it does not satisfy constitutional law. 137

(bb) Based on these standards, electronic profiling is not permissible as a purely precautionary measure before a specific danger arises, since it would result in interferences with fundamental rights that potentially concern highly sensitive personal information without requiring any grounds for suspicion while indiscriminately affecting a large number of persons. 138

Compared to other purely precautionary investigation measures relating to individuals that the Federal Constitutional Court considered not to be impermissible from the outset, electronic profiling under the NRW Police Act differs in that it does not require any facts-based connection between a threat situation and a person specifically responsible for it for that person becoming the potential target of investigation. As a measure to “identify persons of interest”, electronic profiling neither serves to further investigate specific persons suspected of criminal conduct (cf. in this respect BVerfGE 107, 299 <314 *et seq*., 326 *et seq*.>), nor to further consolidate a suspicion, established by other means, that certain persons pose a threat [to protected legal interests] (cf. in this respect BVerfGE 100, 313 <395>; 110, 33 <58 *et seq*., 61>; 113, 348 <375 *et seq*., 378 *et seq*., 383>). 139

The Federal Constitutional Court has emphasised the requirement deriving from the rule of law that in cases where neither a suspicion that a person is responsible for a danger to public security nor a criminal suspicion has been established, it is still nec- 140

essary to establish a sufficient factual basis showing a connection between persons affected by the measure and possible violations of legal interests. In the case of electronic profiling, this requirement is rendered meaningless, as this measure does not in any way require that a chain of factual evidence be established, pointing to at least somewhat specific grounds for suspicion of criminal conduct relating to an individual. It follows that there are shortcomings in terms of the rule of law, given that electronic profiling typically does not require a sufficiently close connection between the threatened legal interest the measure aims to protect and the persons affected by the interference with fundamental rights resulting from the measure; these shortcomings must be compensated in other ways in order to ensure that the authorisation to carry out this measure does not become devoid of any limitation. In the case at hand, the legislator chose not to define the electronic profiling measures authorised for protecting the relevant legal interests in such a way that possible interferences with fundamental rights resulting therefrom do not result in notable impairments for the persons affected by the measure. Nor did the legislator subject the power to carry out the interferences to strictly limited grounds. This is only compatible with the constitutional requirements if the statutory authorisation at least requires a specific danger to the respective legal interest as prerequisite for carrying out the measure.

(cc) Under constitutional law, the statutory threshold for carrying out electronic profiling measures does not necessarily have to be the requirement of a present danger in the traditional sense; however, as a minimum threshold, the statutory authorisation must at least require the existence of a specific danger. 141

(α) § 31 of the 1990 NRW Police Act sets forth the requirement of a present danger, which is the traditional statutory element [of police law] limiting, in line with the rule of law, the extent to which measures may affect persons that are not themselves responsible for a danger to public security. A danger is qualified as a present one when the damage resulting from a hazardous event has already begun to materialise or when such damage can be expected, in all probability, to occur immediately or in the very near future [...]. This satisfies the constitutional requirements regarding the statutory authorisation of electronic profiling. 142

Nevertheless, the requirement of a present danger in that sense is not a necessary prerequisite under constitutional law [with regard to electronic profiling]. It is true that it cannot be ruled out from the outset that electronic profiling might actually yield results within a short period of time in individual cases. Even so, in light of the efforts regularly required to carry out electronic profiling, the statutory requirement that damage will, in all probability, occur in the very near future means that in most cases where this requirement is satisfied, electronic profiling would be too late to be effective. Given the high standing of the legal interests set forth in § 31(1) of the 1990 NRW Police Act, such a far-reaching restriction of electronic profiling as a search measure is not necessary to ensure proportionality. 143

(β) Rather, it is sufficient that the legislator ties the permissibility of electronic profil- 144

ing to the requirement of a specific danger to the legal interests in question. This means that there must be a situation where it is sufficiently likely, in the individual case, that damage to the protected legal interests will occur in the foreseeable future (cf., e.g., § 2(1) no. 1 lit. a of the Lower Saxony Public Security and Order Act). However, under constitutional law, the state bodies responsible for applying such a statutory authorisation are barred from interpreting the term ‘danger’ under police law in a way that disregards these requirements, which would lower the danger threshold [justifying the interference] to one that is below the constitutionally required minimum threshold for electronic profiling.

The probability prognosis required for establishing a specific danger must be based on facts. Vague indications or mere assumptions without tangible grounds relating to the individual case are not sufficient (cf. BVerfGE 44, 353 <381 and 382>; 69, 315 <353 and 354>). 145

(γ) A state of permanent danger (*Dauergefahr*) may also fit the elements of a specific danger within that meaning. Such a permanent danger is characterised by a sufficient probability that, over a longer period of time, damage might occur at any point. However, for establishing such a permanent danger, the requirements for establishing a specific danger apply accordingly, namely the requirement of a sufficient probability of damage and the requirement of a specific factual basis for the probability prognosis. 146

Therefore, sufficiently compelling and specific facts are required for establishing a specific permanent danger, for example the danger posed by so-called sleeper terrorists. [...] 147

(δ) Furthermore, making the permissibility of electronic profiling contingent upon the existence of a specific danger is also imperative as it provides the basis for determining the proportionality of electronic profiling in the individual case, and for further specifying the additional procedural and organisational requirements for carrying out the measure, which are not under review here. Without this limitation, it would not be possible to further define these additional requirements in line with the principle of legal specificity deriving from the rule of law. 148

c) The statutory authorisation in § 31(1) of the 1990 NRW Police Act satisfies the constitutional requirement of legal specificity and clarity, provided that its scope of application is understood in the meaning set out here. 149

aa) Authorisations to interfere with fundamental rights require a statutory basis that satisfies the requirement of legal specificity and clarity deriving from the rule of law (cf. BVerfGE 110, 33 <53>). For interferences with the fundamental right to informational self-determination – just as for interferences with the specific fundamental rights of Arts. 10 and 13 of the Basic Law – the legislator must specify precisely, for each subject matter, the purposes for which the data may be used (cf. BVerfGE 65, 1 <46>; 110, 33 <70>; 113, 29 <51>). Pursuant to § 31(1) of the 1990 NRW Police 150

Act, the sharing of data serves to enable the automated cross-checking of the shared data against other data sets, to the extent that this is necessary to avert certain dangers, namely dangers to the existence or security of the Federation or a *Land* or to life, limb or liberty of the person. Thus, the purpose for which the data may be used is the automated cross-checking of the shared data against other data sets to avert the dangers listed in § 31(1) of the 1990 NRW Police Act. This is sufficient.

Provisions governing the sharing of data must satisfy the requirement that the receiving authorities be designated in a sufficiently identifiable manner, along with rules ensuring that data sharing remain concentrated within the scope of the specific tasks assigned to those authorities (cf. in this respect BVerfGE 110, 33 <70>). This requirement is only satisfied if the term ‘danger’ serves to limit the statutory authorisation for data sharing. In the case at hand, the police are designated as the receiving authority for the shared data. The purpose for which the data may be used is limited to averting dangers to specifically listed and high-ranking protected interests of public security, i.e. a purpose that is part of the specific tasks assigned to police authorities (cf. § 1(1) first sentence of the 1990 NRW Police Act). 151

Under the above-mentioned conditions, § 31 of the 1990 NRW Police Act is also sufficiently specific regarding not only the types of data expressly listed, but also to the extent that “other data required in the individual case” may be requested and processed pursuant to § 31(2) of the 1990 NRW Police Act. In this respect, the requirements of legal specificity are met, given that the phrase “other data required in the individual case” can be interpreted more specifically – taking into consideration the legislative purpose of averting danger to public security, which also determines for which purposes “necessary” data may be requested – in such a way that the principle of proportionality is satisfied. 152

bb) By contrast, if measures were not limited by the requirement of a specific danger, there would be no sufficient basis for determining, based on the legislative purpose, what data may be covered by the measure, in particular what data constitutes “other data necessary in the individual case”. Without the element of a specific danger, it cannot be established in a sufficiently specific manner, as required under constitutional law, under which circumstances data is considered “necessary in the individual case”. For instance, if electronic profiling were based on the general threat of terrorism and if this general threat situation thus served as the basis for determining what specific type of data is necessary for the police, the authorisation to use electronic profiling would essentially become devoid of any limitation. […] 153

II.

The challenged decisions do not satisfy the constitutional requirements. They are based on an expansive interpretation of the term ‘present danger’ in § 31(1) of the 1990 NRW Police Act that is contrary to the principles set out above. As a result, the statutory authorisation is transformed into an authorisation conferring precautionary 154

powers. This interpretation assigns a meaning to this provision that even the legislator could not have adopted without violating the fundamental right to informational self-determination under Art. 2(1) in conjunction with Art. 1(1) of the Basic Law.

1. It is true that the interpretation of statutory law and its application to the specific case fall to the competent ordinary courts and are generally not subject to review by the Federal Constitutional Court (established case-law; cf. BVerfGE 18, 85 <92 and 93>). The interpretation adopted by the ordinary courts, however, must be guided by the affected fundamental rights to ensure that the values enshrined therein are upheld when applying the relevant statutory provisions (established case-law; cf. BVerfGE 7, 198 <205 *et seq*.>; 101, 361 <388>). When ordinary courts interpret the scope of application of a statutory provision expansively, thereby assigning a meaning to that provision that even the legislator could not have adopted without violating fundamental rights, and the courts then base the application of that provision in the specific case on such an interpretation, they fail to recognise the significance and scope of fundamental rights (cf. BVerfGE 81, 29 <31 and 32>; 82, 6 <15 and 16>). 155

2. This is what the courts did in the case at hand. In the challenged decisions, the courts interpret the term ‘present danger’ in § 31(1) of the 1990 NRW Police Act in a manner that does not satisfy the constitutional requirements applicable to statutory provisions authorising electronic profiling, specifically the requirement that there be at least a specific danger. 156

a) The electronic profiling measures that were coordinated across Germany after 9/11 required the courts to take decisions in the context of a novel threat situation. This led to uncertainty with respect to handling the statutory basis authorising such measures. Some of the courts deciding on these electronic profiling measures held on to the traditional understanding of the term ‘present danger’ and found that a present danger did not exist in the cases before them [...]. In light of the magnitude of possible damage, however, other courts lowered the standard establishing the required probability of damage and, based on this standard, found the existence of a present danger [...]. This is also what the courts in the challenged decisions did. The underlying interpretation of § 31(1) of the 1990 NRW Police Act does not satisfy the constitutional requirements. 157

b) The challenged decisions do not take into account that ordering electronic profiling is only permissible under constitutional law if it is subject to the existence of at least a specific danger and if the required degree of probability that a violation of legal interests will occur is established by taking into consideration not only the magnitude of possible damage, but also the weight of the interference resulting from the measure carried out to avert the relevant danger as well as its prospects of success. Based on the constitutional standards outlined above, electronic profiling may only interfere with the fundamental right to informational self-determination of a complete non-suspect if the existence of a danger can be established based on specific facts, giving rise to the assumption that measures can be taken on the basis of the investi- 158

gation of data of a certain group of persons that contribute to averting this danger.

[…] 159-160

Contrary to constitutional law, the courts completely dispensed with the requirement that there must be a specific danger, i.e. danger in the individual case and based on sufficient facts, by lowering the threshold of probability to the mere [general] possibility of terrorist attacks. The courts did so by qualifying this [general] threat situation as a ‘danger’, thus assigning a meaning to this term that under constitutional law is not a sufficient basis for authorising electronic profiling. 161

3. The challenged decisions are informed by these constitutional shortcomings as it can reasonably be assumed that the courts would have reached a different conclusion if they had observed the constitutional requirements for interpreting the term ‘present danger’ in § 31(1) of the 1990 NRW Police Act. 162

III.

[…] 163

IV.

[…] 164-165

With regard to B II., the decision was taken with 6:2 votes; for the rest it was unanimous. 166

Papier Haas Hömig

Steiner Hohmann-Dennhardt Hoffmann-Riem

Bryde Gaier

Dissenting Opinion of Justice Haas

I do not agree with the decision of the Senate majority to the extent that it holds the Higher Regional Court's order to be unconstitutional and reverses it. The Higher Regional Court's interpretation and application of § 31(1) of the 1990 NRW Police Act is not objectionable under constitutional law. [...] I agree with the Senate majority on the finding that § 31(1) of the 1990 NRW Police Act is constitutional, albeit for other reasons. 167

1. The Senate majority and the challenged decision by the Higher Regional Court correctly assume that § 31(1) of the 1990 NRW Police Act interferes with Art. 2(1) in conjunction with Art. 1(1) of the Basic Law. However, this holds true only with regard to data obtained on the basis of § 31(1) of the 1990 NRW Police Act that is not immediately deleted in an automated procedure (cf. BVerfGE 100, 313 <366>; 107, 299 <328>). This means that the fundamental rights of the vast majority of persons whose data was used in the electronic profiling measures were not affected. 168

Moreover, the case at hand shows that even for the rest of the persons whose data is obtained and cross-checked, the interference is minor [...]. 169

In my view, it is significant for assessing the severity of the interference that the authorisation to obtain and cross-check data on the basis of § 31(1) of the 1990 NRW Police Act only extends to data that has already been disclosed by the affected persons and is stored in databases. In this respect, it must be taken into account that the weight of the interference can only be assessed when considering the criteria on which the profile used in the specific measure was based, given the diversity of threat situations. In addition, information such as sex, place of residence, parenthood, field of study are accessible to anyone anyhow. Anyone can obtain knowledge of these attributes and life circumstances by observing the persons concerned and questioning persons in their social environment. Likewise, it is possible for the state to obtain such knowledge and use it, yet this does not necessarily amount to a particularly serious interference with the individual's general right of personality in each and every case. This holds true all the more where the data concerned has been disclosed specifically to state bodies by the affected persons themselves or where state bodies have recorded the data – in the interest of the affected persons – for other reasons, as is the case here. 170

This also applies to a person's religion, in particular with regard to Muslims, who in general practice their faith openly and, in our free state, do not suffer disadvantages for it. [...] Contrary to the Senate majority's opinion, it cannot be claimed that the affected persons have particular expectations of privacy and confidentiality regarding their place of residence and the religion they practice, as this data is usually made public by the affected persons themselves. Despite what the Senate majority believes, there are no stigmatising effects resulting from cross-checking data on religious affiliation, given that electronic profiling is not carried out in public and thus will generally not become public knowledge. Moreover, we underestimate citizens if we 171

assume that they would perceive the police measure in this way. […]

The interference cannot be regarded as particularly intrusive merely because data from a large number of persons is obtained and cross-checked. In each case, the interference only affects the respective individual. Therefore, the severity of interference is determined by how intrusive the measure is for that individual. Whether other persons are also affected by the measure neither mitigates nor aggravates the intensity of the interference for the individual person. In addition, and contrary to the Senate majority's opinion, the fact that a large amount of data is used in the cross-checking actually works to the advantage of the affected fundamental rights holders, given that they *de facto* remain anonymous despite their names being entered into the system. Not least due to the overall volume of data, the entirety of the data records is inscrutable. Therefore, the data subjects do not stand out as individual persons and thus *de facto* remain anonymous. It is only when the number of data subjects is narrowed down to a lower figure (less than a hundred in the case at hand) that data subjects are perceived as individual persons in the context of specific checks. This is decisive for determining the severity of the interference. Thus, as long as the group of data subjects affected by electronic profiling is considerably large, the interference can from the outset not be qualified as particularly intrusive. 172

2. The circumstances of the interference that the Senate majority took into consideration do not suffice, neither separately nor in an overall assessment, to convincingly establish an interference of high intensity; regardless of this, the majority opinion fails to consider one aspect of electronic profiling authorised under § 31(1) of the 1990 NRW Police Act that is absolutely decisive in my view: by merely obtaining data that the state had already collected separately and thus had readily at its disposal anyway, the state safeguards and strengthens freedom, including in particular the freedom of persons affected by the data cross-checking. Therefore, the measure primarily serves to safeguard and strengthen freedom. 173

The fundamental right to freedom requires that the state guarantee security. Without security, the Basic Law's guarantee of freedom rings hollow. [...] In a democratic state under the rule of law, more security strengthens freedom, thus increasing freedom. This holds true even with regard to citizens whose freedom is affected by state measures serving prevention and protection purposes – state measures touching on their right to decide themselves on the use of their personal data – and who did not themselves prompt the presumption that they seek to impair or destroy the lives of fellow citizens. [...] 174

The state must take seriously the fear for one's life and health. [...] By fulfilling its mandate of protection, the state does not limit the freedom of its citizens; rather, it strengthens and safeguards their right to freedom. 175

When individuals are free from fear, they are free to act in self-determination, to develop their personality and thus their abilities. Contrary to the Senate majority's opinion, the cross-checking of data, carried out in a matter of seconds, does not control 176

or inhibit behaviour. Affected persons will not change their behaviour because of it. [...] The arguments developed in the context of telecommunications surveillance cannot be applied to electronic profiling. This holds true all the more as, given the type of data used, the cross-checking of data carried out in the context of electronic profiling is not repeated on a daily or weekly basis; unlike surveillance of telecommunications, it is not a measure continuously carried out over a certain period of time, targeting the contents of interpersonal communication and thus the confidential sphere from which novel, previously unknown information is gathered.

[…] 177

3. It does not raise constitutional concerns that § 31(1) of the 1990 NRW Police Act, which, in conjunction with the principle of proportionality, provides the statutory basis for electronic profiling, requires the existence of a present danger. However, the element of present danger alone would not constitute a suitable criterion for determining when to allow electronic profiling measures. If it were not possible to launch electronic profiling measures until the danger was already present, electronic profiling would simply be a useless investigation method. [...] 178

Art. 31(1) of the 1990 NRW Police Act requires the existence of a present danger. This is compatible with constitutional law if, in accordance with case-law and legal scholarship, the notion of reverse proportionality is taken into account when interpreting the provision. This entails that the principle of proportionality must be taken into account when making the necessary prognosis as to how likely it is that damage will occur; accordingly, a differentiation must be made based on the magnitude of possible damage [...]. Thus, the greater the possible damage, the lower the requirements regarding the probability of damage occurring may be for the purposes of authorising police measures. [...] This enables the police to already take precautionary measures in order to prevent criminal acts and thus avert risks, to which the Basic Law itself accords great importance (cf. BVerfGE 100, 313 <388>; most recently BVerfGE 115, 166 <192>). 179

[…] 180

4. The Higher Regional Court was right to find the existence of a terrorist threat in the challenged decision based on the factual indications in the present case, which justified electronic profiling. These circumstances were not accorded the significance they deserve by the Senate majority. [...] Given the threat to a large number of innocent people, it was permissible for that court to hold that the complainant’s interests and the interference with his right to informational self-determination, which cannot be qualified as serious, carry less weight than the security interests of all citizens and the state’s mandate of protection. As citizens connected to and bound by the community, the persons affected by electronic profiling have to tolerate, in the interest of the general public, the interference of minor weight at issue here. 181

5. […] 182-184

Haas

Bundesverfassungsgericht, Beschluss des Ersten Senats vom 4. April 2006 - 1 BvR 518/02

Zitiervorschlag BVerfG, Beschluss des Ersten Senats vom 4. April 2006 - 1 BvR 518/02 - Rn. (1 - 182-184), http://www.bverfg.de/e/rs20060404_1bvr051802en.html

ECLI ECLI:DE:BVerfG:2006:rs20060404.1bvr051802