Headnotes

to the Judgment of the First Senate of 16 February 2023

- 1 BvR 1547/19 -
- 1 BvR 2634/20 -

Automated data analysis

1. **When stored data is processed by means of automated data analysis or interpretation, this constitutes an interference with the informational self-determination (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law) of anyone whose personal data is used in such processing.**

2. **The severity of interference resulting from automated data analysis or interpretation and the requirements regarding their justification under constitutional law are partly determined by the severity of interference resulting from the preceding collection of the data; in this respect, the principles of purpose limitation and change in purpose apply. Moreover, automated data analysis or interpretation amount to a separate interference because the further processing of data can result in specific detrimental effects which might be more onerous than the severity of interference resulting from the original data collection; in this respect, the principle of proportionality in the strict sense requires that additional justification be provided.**

3. **These more extensive requirements for the justification of automated data analysis or interpretation are variable given that the severity of interference can differ substantially depending on the design of the statutory framework. The severity of interference primarily depends on the type and scope of the usable data and the permitted methods of data analysis or interpretation. The legislator can control the severity of interference by providing for rules on the type and scope of the usable data and by limiting the permissible methods of analysis.**

4. If automated data analysis or interpretation give rise to serious interferences with the informational self-determination of affected persons, such interferences can only be justified subject to the strict requirements that apply to intrusive covert surveillance measures generally. This means that the use of such methods is only permissible to protect particularly weighty legal interests for which there is at least a sufficiently identifiable danger. The threshold of an at least identifiable danger to particularly weighty legal interests may only be constitutionally dispensed with if the regulatory framework, in a clear and sufficiently specific manner, limits the permissible options of data analysis or interpretation so narrowly that the severity of interference resulting from the measures is substantially reduced. This can primarily be achieved by setting out rules limiting the type and scope of the usable data and restricting the permissible methods of data processing.

5. In principle, the legislator may divide the task of setting out such rules, laying down some elements itself while allowing other rules to be determined by the administrative authorities. However, the legislator must ensure that the rules are sufficient as a whole and comply with the requirement that interferences be based on statutory provisions.

a. The legislator itself must provide for the basic legal framework limiting the type and scope of usable data and the permissible data processing methods.

b. Insofar as the legislator authorises the administrative authorities to issue detailed organisational and technical rules, the legislator must ensure that the administrative authorities lay down the requirements and criteria applicable to automated data analysis or interpretation in the individual case in an abstract and generalised manner, that they ensure reliable documentation, and that they publish their determinations in a form to be specified by the legislator. This also serves to guarantee the constitutionally required oversight, which can be exercised in particular by data protection officers.

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 1547/19 -

- 1 BvR 2634/20 -

Pronounced
on 16 February 2023
Hoffmann
Regierungshauptsekretär
as Registrar
of the Court Registry

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaints

I. of [5 complainants]

– authorised representatives: 1.Prof. Dr. Tobias Singelnstein,
(...)
- authorised representative for nos. 1 to 5 -

2.Rechtsanwältin Sarah Lincoln,
(...)
- authorised representative for no. 3 -

against § 25a of the Security and Public Order Act for the *Land* Hesse as amended by the Intelligence Service Restructuring Act of the *Land* Hesse of 25 June 2018 ([...]).

- 1 BvR 1547/19 -,

II. of [6 complainants]

– authorised representatives: 1.Jun.-Prof. Dr. Sebastian Golla,
Universitätsstraße 150, 44801 Bochum
- authorised representative for nos. 1 to 6 -

2.Rechtsanwalt Dr. Bijan Moini,
(...)
- authorised representative for no. 6

against § 49 of the Act on Data Processing by the Police for the *Land* Hamburg as amended by the Act on Data Processing by the Police and Amending Other Police Law Provisions of 12 December 2019 ([...]).

- 1 BvR 2634/20 -

the Federal Constitutional Court – First Senate –

with the participation of Justices

President Harbarth,

Baer,

Britz,

Ott,

Christ,

Radtke,

Härtel,

Wolff

held on the basis of the oral hearing of 20 December 2022:

Judgment:

1. § 49(1) first alternative of the Act on Data Processing by the Police for the *Land* Hamburg as amended by the Act on Data Processing by the Police and Amending Other Police Law Provisions of 12 December 2019 ([...]) violates Art. 2(1) in conjunction with Art. 1(1) of the Basic Law and is void.

In all other respects, the constitutional complaint in proceedings 1 BvR 2634/20 is rejected.

The Free and Hanseatic City of Hamburg must reimburse two-thirds of the necessary expenses incurred by the complainants in the constitutional complaint proceedings 1 BvR 2634/20.

2. § 25a(1) first alternative of the Security and Public Order Act for the *Land* Hesse as amended by the Intelligence Service Restructuring Act of the *Land* Hesse of 25 June 2018 ([...]) is incompatible with Art. 2(1) in conjunction with Art. 1(1) of the Basic Law.

Until the legislator has enacted new provisions, or until 30 September 2023 at the latest, § 25a(1) first alternative of the Security and Public Order Act continues to apply subject to the following conditions: Police in Hesse are only permitted to conduct data analysis under § 25a(1) first alternative of the Security and Public Order Act on condition that sufficiently specific facts give rise to the suspicion that a particularly serious criminal offence within the meaning of § 100b(2) of the Code of Criminal Procedure has been committed and it is expected, given the particular circumstances of the suspicion in the individual case, that similar criminal offences will be committed that will jeopardise the life and limb of persons or the existence or security of the Federation or a *Land*. Furthermore, the existence of these requirements and the specific suitability of the data used to prevent the expected criminal offence must be confirmed in a written explanation in each individual case; it must also be ensured that no information is used that was obtained from the surveillance of private homes, remote searches, telecommunications surveillance, traffic data retrieval, longer-term observations, the use of undercover investigators or confidential informants, or from similarly serious interferences with the right to informational self-determination.

In all other respects, the constitutional complaint in proceedings 1 BvR 1547/19 is rejected.

The *Land* Hesse must reimburse two-thirds of the necessary expenses incurred by the complainants in the constitutional complaint proceedings 1 BvR 1547/19.

Table of contents

Reasons:

A.

The constitutional complaints are directed against provisions of *Land* law that authorise the police to conduct automated data analysis or interpretation. 1

I.

§ 25a of the Security and Public Order Act for the *Land* Hesse (*Hessisches Gesetz über die öffentliche Sicherheit und Ordnung* – HSOG; hereinafter: the Hesse Act) as amended by the Intelligence Service Restructuring Act of the *Land* Hesse (*Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen*) of 25 June 2018 ([...]) and § 49 of the Act on Data Processing by the Police for the *Land* Hamburg (*Hamburgisches Gesetz über die Datenverarbeitung der Polizei* – HmbPolDVG; hereinafter: the Hamburg Act) as amended by the Act on Data Processing by the Police and Amending Other Police Law Provisions (*Gesetz über die Datenverarbeitung der Polizei und zur Änderung weiterer polizeirechtlicher Vorschriften*) of 12 December 2019 ([...]) essentially have the same wording. In view of the expanded technical possibilities for using information technology in police work, these provisions establish a specific legislative basis for linking previously unconnected, automated databases and data sources within analysis platforms and for systematically mining the available datasets through searches, thereby enabling the police to carry out their tasks more efficiently and effectively ([...]). 2

The provisions authorise the police, in justified individual cases, to process stored personal data using automated data analysis (Hesse) or automated data interpretation (Hamburg) – either as a precautionary measure for the prevention of serious criminal offences within the meaning of § 100a(2) of the Code of Criminal Procedure (*Strafprozessordnung* – StPO) (first alternative) or for the purpose of averting a danger to certain legal interests (second alternative). Pursuant to section (2) of both provisions, relationships or connections between persons, groups of persons, institutions, organisations, objects or matters can thereby be established, insignificant information and intelligence can be filtered out, generated insights can be matched to known facts, and stored data can be statistically analysed. [...] 3

II.

[...] 4-5

III.

With the introduction of § 25a of the Hesse Act, powers to conduct automated data analysis were for the first time set out in *Land* law. The legislator thereby created a statutory framework for police activities that were already established in practice. The powers granted under § 25a of the Hesse Act are used thousands of times each year. Although largely modelled on § 25a of the Hesse Act, § 49 of the Hamburg Act has yet to be applied. 6

1. In 2017, the *Land* Hesse purchased the 'Gotham' operating system from the software company Palantir and ran it under the name 'hessenDATA'. In 2018, the *Land* legislator decided to create a separate legal basis especially for this application, primarily to ensure that the right to informational self-determination was properly taken into account ([...]). 7

The explanatory memorandum to the draft version of § 25a of the Hesse Act suggested that without the help of such automated systems, valuable indications of dangers and imminent criminal offences would go undetected in the police IT environment due to the uncoordinated coexistence of various automated processes, datasets and information systems all working independently of one another, each with their own unique purpose limitations, authorised users, types of data and target persons. Problems with the flow of information had become particularly evident during the nationwide series of murders carried out by the 'NSU' group. [...] 8

As the explanatory memorandum stated, § 25a of the Hesse Act applies to the automated analysis of personal data that has already been lawfully obtained. It also stated that the general rules contained in § 20 of the Hesse Act on further processing, purpose limitation and the principle of a hypothetical recollection of data must be observed, as must special rules on data use. What datasets are to be used in each particular case must be assessed on the basis of the purpose of the given data analysis. If necessary, access to the data must be controlled by means of user authorisations ([...]). 9

[...] 10

The Interior Minister of the *Land* Hesse explained that the analysis platform had automated access to three databases: POLAS (a police information system containing 'repressive' law enforcement data), ComVor (a case management system for all proceedings) and CRIME-ST (a case management system designed to store 'preventive' data for future investigations) ([...]). The relevant data was automatically transferred to the analysis platform and synchronised at regular intervals, which had the added effect of ensuring compliance with deletion deadlines ([...]). Other sources used by the platform included traffic data from telecommunications surveillance and from retrieval queries (including radio cell queries). Data obtained from 'forensic extraction' (e.g. from mobile phones seized by the police) was also analysed. Use was also made of data from police telexes – a kind of e-mail system used by the police to exchange information throughout the *Land* Hesse ([...]). The source systems of other *Länder*, the Federation and foreign states were not automatically integrated, nor were any other public or non-public sources. However, this could be requested (within the statutory limits) and the relevant sources could then be integrated into the platform and analysed. The same applied, in individual cases, to data from police investigation measures carried out for preventive purposes and to data from criminal investigation measures (such as the surveillance of telecommunications or private homes). Subject to the requirement of a prior court order, it also applied to data from social networks. The analysis platform did not have direct access to social networks because security reasons prevented the police IT system from di- 11

rectly accessing the internet. No use was made of data from the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*) or the *Land* Offices for the Protection of the Constitution (*Landesämter für Verfassungsschutz*) ([...]).

The hessenDATA analysis platform was integrated into the police network and, if required, could be accessed from any workstation in Hesse. However, the stored datasets could only be accessed and used by police officers with special training, the majority of whom were criminal investigators. Access to the data was controlled by a role and rights-based concept. Users of the platform were assigned to different groups, each group having different access rights to the integrated data. [...] At the oral hearing, the Hessian Ministry of the Interior and Sports stated that 2,099 persons currently had access to hessenDATA. The platform was used in around 14,000 cases each year. In 2,000 of these cases, data analysis was carried out under § 25a(1) second alternative of the Hesse Act (i.e. for the purpose of averting a danger to certain legal interests), while in 12,000 cases it was carried out under § 25a(1) first alternative of the Hesse Act (i.e. as a precautionary measure for the prevention of specific criminal offences). 12

2. As part of the Act on Data Processing by the Police for the *Land* Hamburg that was newly created by the Act on Data Processing by the Police and Amending Other Police Law Provisions ([...]), § 49 of the Hamburg Act came into effect on 24 December 2019. Its draft version was heavily based on § 25a of the Hesse Act. However, one difference from the outset was that § 49(1) of the Hamburg Act describes the stored personal data that may be subjected to automated processing as data stored in 'police filing systems', whereas § 25a of the Hesse Act simply refers to stored data. [...] 13

In the final version of the Hamburg Act, the term 'data analysis' (*Datenanalyse*), which appeared in the draft version (and was retained in the final version of the Hesse Act), was replaced by the term 'data interpretation' (*Datenauswertung*). This was primarily to emphasise that automated data processing did not involve the autonomous evaluation of content via intelligent and possibly even self-learning algorithms ([...]). [...] 14

[...] 15

IV.

[...] 16

In both sets of proceedings, the complainants allege that the challenged provisions – § 25a of the Hesse Act and § 49 of the Hamburg Act respectively – interfere disproportionately with their fundamental right to informational self-determination (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law). They furthermore claim a violation of the fundamental right to the inviolability of the home under Art. 13(1) of the Basic Law and a violation of the privacy of telecommunications under Art. 10(1) of the Basic Law insofar as automated data analysis/interpretation makes use of personal data from the surveillance of private homes or telecommunications. In proceedings 1 BvR 1547/19, the complainants also claim that the confidentiality and integrity of IT systems guaranteed by Art. 2(1) in conjunction with Art. 1(1) of the Basic Law is violated to the extent that 17

data obtained from remote searches of IT systems is used. Furthermore, both constitutional complaints argue that deficiencies in the challenged provisions and the accompanying rules amount to a violation of the fundamental right to effective legal protection under Art. 19(4) of the Basic Law.

[...] 18-22

V.

In proceedings 1 BvR 1547/19, statements were submitted by the Hessian State Chancellery (*Hessische Staatskanzlei*) and the Hessian Officer for Data Protection and Freedom of Information (*Hessische Beauftragte für Datenschutz und Informationsfreiheit*). In proceedings 1 BvR 2634/20, statements were submitted by the Hamburg Ministry of Justice and Consumer Protection (*Behörde für Justiz und Verbraucherschutz der Freien und Hansestadt Hamburg*) and the Hamburg Officer for Data Protection and Freedom of Information (*Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*). The Federal Officer for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) submitted statements in both proceedings. 23

[...] 24-45

VI.

At the oral hearing on 20 December 2022, the Federal Constitutional Court heard the complainants along with the *Land* Government of Hesse and the Government of the Free and Hanseatic City of Hamburg. The Hessian Officer for Data Protection and Freedom of Information, the Hamburg Officer for Data Protection and Freedom of Information, and the Federal Officer for Data Protection and Freedom of Information were heard as expert third parties in accordance with § 27a of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz* – BVerfGG), as was Dr. Constanze Kurz speaking on behalf of the *Chaos Computer Club e.V.* 46

B.

The constitutional complaints directed against § 25a of the Hesse Act and § 49 of the Hamburg Act are only admissible to the extent that they are directed against the threshold for interference established in § 25a(1) first alternative of the Hesse Act and in § 49(1) first alternative of the Hamburg Act (automated data analysis/interpretation as a precautionary measure for the prevention of criminal offences). [...] 47

For the rest, the constitutional complaints are inadmissible. The Federal Constitutional Court's review is not therefore concerned with the question of whether the legislators enacted constitutionally sufficient provisions in respect of the legal interests to be protected by data analysis/interpretation under § 25a of the Hesse Act and § 49 of the Hamburg Act. Nor does the Court need to examine whether the procedural and organisational rules designed to ensure transparency and legal protection meet the constitutional requirements, nor whether the procedural safeguards in place are sufficient given the 48

complex forms of automated data matching and self-learning systems (artificial intelligence/AI) that now exist. Nor does it have to examine whether the constitutional principle of the purpose limitation applicable to previously collected personal data has been complied with, in particular whether sufficient limits have been placed on the ability to make further use of data obtained from interferences with Art. 13(1) or Art. 10(1) of the Basic Law. The complainants have not sufficiently demonstrated the possibility of a violation of fundamental rights in this respect. [...]

C.

Insofar as the constitutional complaints are admissible, they are well-founded. The challenged powers can at any rate lead to interferences with the right to informational self-determination (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law) as a manifestation of the general right of personality (see I. below). In principle, interferences with fundamental rights arising from automated data analysis/interpretation by police authorities are justifiable under constitutional law. The constitutional requirements for the justification of automated data analysis/interpretation depend on the specific reach of the powers in question and are thus variable; here they are strict due to the design of the challenged provisions (see II. below). In light of the foregoing, §25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act do not contain sufficient thresholds for interference (see III. below). Both provisions are therefore unconstitutional insofar as they authorise data analysis/interpretation to be conducted as a precautionary measure for the prevention of criminal offences. The powers to conduct data analysis/interpretation for the purpose of averting a danger to certain legal interests (§ 25a(1) second alternative of the Hesse Act, § 49(1) second alternative of the Hamburg Act) remain unaffected. 49

I.

When stored data is processed by means of automated data analysis/interpretation in accordance with § 25a of the Hesse Act or § 49 of the Hamburg Act, this constitutes an interference with the informational self-determination (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law) of anyone whose personal data is used in such processing. By authorising the automated analysis/interpretation of stored data, the legislator permits the further use of previously collected data beyond the grounds that prompted the original data collection. This constitutes a separate interference with fundamental rights and must be separately justified under constitutional law in accordance with the principle of purpose limitation (cf. Decisions of the Federal Constitutional Court, *Entscheidungen des Bundesverfassungsgerichts* – BVerfGE 141, 220 <324 para. 277, 327 para. 285>; for more details see para. 55 ff. below). However, it is not merely the joining and further use of previously unconnected data that amounts to an interference with fundamental rights – fundamental rights can also be affected by the new intelligence that automated data analysis/interpretation is capable of generating (cf. BVerfGE 156, 11 <39 f. para. 73 f.>; for more details see para. 67 ff. below). 50

II.

In order to be justified, interferences with fundamental rights must be based on a statutory authorisation that pursues a legitimate purpose and also satisfies the principle of proportionality in all other respects. 51

In light of developments in information technology, the challenged provisions serve the legitimate purpose of increasing the effectiveness of precautionary measures to prevent serious criminal offences by making it possible to discover indications of imminent serious crimes that might otherwise remain undetected in the police data. In the present proceedings, the *Land* Government of Hesse demonstrated that, due to the increasing use of digital media and means of communication, particularly in the areas of terrorist and extremist violence and in organised and serious crime, police authorities are faced with ever larger streams of data that are increasingly heterogeneous in terms of quality and format. According to the *Land* Government, automated data analysis is essential for successful police action, since information on these crimes is difficult to obtain through a conventional search of police data records, let alone under time constraints. 52

The provisions are suitable under constitutional law to increase the effectiveness of precautionary measures to prevent criminal offences. They are also necessary in that automated data analysis/interpretation is capable of generating relevant intelligence for the prevention of crime that cannot be generated in an equally effective manner by other, less intrusive means. 53

Special requirements arise here from the principle of proportionality in the strict sense. How stringent these requirements are in each case depends on the severity of interference resulting from the measure in question (cf. BVerfGE 141, 220 <269 para. 105>; 155, 119 <178 para. 128> – *Subscriber data II*; Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 152; established case-law). The severity of interference resulting from automated data analysis/interpretation and the requirements regarding its justification under constitutional law are determined by the severity of interference associated with the preceding collection of data; in this respect, the principles of purpose limitation and change in purpose apply (see 1. below). Furthermore, automated data analysis/interpretation can potentially constitute a separate interference, with the result that justification is subject to additional requirements (see 2. below). 54

1. Under § 25a of the Hesse Act and § 49 of the Hamburg Act, automated data analysis/interpretation is used to further process personal data that was collected and stored at some earlier stage. The justification requirements applicable to the further use of data collected by the state are informed by the principles of purpose limitation and change in purpose (foundationally, BVerfGE 65, 1 <46>). If the legislator permits a use of data beyond the specific grounds that prompted the original data collection and beyond the reasons that justified the original data collection, it must create a separate statutory basis to that end. Provided that the particular constitutional requirements are adhered to, the legislator may authorise the further use of the data within the scope of the purpose 55

for which the data was originally collected (see a) below) and may also allow a change in purpose (see b) below) (cf. BVerfGE 141, 220 <324 ff. para. 276 ff.> with further references; established case-law). § 25a of the Hesse Act and § 49 of the Hamburg Act permit the further use of data not only for purposes in line with the original purpose but also for changed purposes (see c) below).

a) The legislator may allow the use of data beyond the specific investigation that originally prompted the data collection if the contemplated use still falls within the scope of the purpose for which the data was originally collected; in such cases, the legislator is subject to the constitutional requirements applicable to further use within the scope of the original purpose, as fleshed out in the judgment on the Federal Criminal Police Office (cf. BVerfGE 141, 220 <324 ff. para. 278 ff.> with further references). 56

The permissible scope of such use depends on the statutory authorisation for the original data collection. The respective statutory basis determines the authority that is authorised to collect the data, as well as the purposes and conditions of data collection, thereby defining the permissible scope of use. Accordingly, the use of the resulting information is not only limited to certain abstractly defined public tasks but is actually subject to a purpose limitation determined by the collection purpose set out in the relevant statutory basis authorising the respective data collection. For that reason, further uses of data within the scope of the purpose for which the data was originally collected are only permissible if the data is used by the same authority in relation to the same task and for the protection of the same legal interests as was the case with regard to the data collection. If the original authorisation to collect data is restricted to the purpose of protecting specified legal interests or preventing specified criminal offences, this purpose limits both the scope of immediate data use and the scope of further data uses, even if the data is still handled by the same authority. Other uses are only permissible if there is a separate statutory basis authorising such a change in purpose. 57

In principle, the purpose limitations that the same authority must observe whenever it makes further use of collected data while acting within the same remit for the protection of the same legal interests do not include the relevant thresholds for exercising the data collection powers – this holds true for the threshold of a sufficiently identifiable danger (*hinreichend konkretisierte Gefahr*) as is traditionally required for public security measures, and the threshold of a qualified suspicion of criminal conduct (*qualifizierter Tatverdacht*) as is required in the context of law enforcement. While the requirement of establishing a sufficiently identifiable danger or a qualified suspicion of criminal conduct determines the permissible grounds of data collection, it does not determine the purposes for which the collected data may be used. For that reason, it does not from the outset run counter to the principle that data be used only in accordance with the purpose for which it was originally collected if the authority in question is allowed to consider the data as providing leads for further investigations within the same task, without having to fulfil additional prerequisites. The authority may use the information thus obtained – either by itself or in combination with other available information – as a starting point for further investigations to protect the same legal interests in the context of the 58

same task. This does not create an opening for purely speculative uses of data, because using the data to provide leads for further investigations is still sufficiently linked to the original investigation due to the principle of purpose limitation – which limits the purpose of further use to the tasks involved in the original data collection – and due to the requirements concerning the legal interests to be protected. The principle of purpose limitation is satisfied if the authority that is authorised to collect data makes further use of this data while acting within the same remit for the protection of the same legal interests and for the prosecution or prevention of the same criminal offences, as specified in the statutory provision authorising the data collection. These requirements are necessary, but generally also sufficient, to legitimise further use of the data in accordance with the principle of purpose limitation.

59 With data obtained from the surveillance of private homes and remote searches of information technology systems, however, the principle of purpose limitation gives rise to more stringent requirements. Any further use of such data, including by the same authority acting within the same remit for the protection of the same legal interests and for the prosecution or prevention of the same criminal offences, only satisfies the purpose limitation requirements if this further use is necessary to avert an acute danger (*dringende Gefahr*) (cf. Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 297 with further references) or at least a sufficiently identifiable danger in the individual case (cf. BVerfGE 141, 220 <272 f. para. 112>), in keeping with the prerequisites applicable to the original collection of such data. The extraordinary severity of interference resulting from this type of data collection is reflected in a particularly narrow limitation of any further use of the obtained data, which is subject to the prerequisites and purposes specified for the original data collection. Intelligence obtained from the surveillance of private homes and remote searches may not be used to provide leads for further investigations unless there is an acute danger or at least a sufficiently identifiable danger in the individual case.

60 b) The legislator may also allow further uses of the data for purposes other than those for which the data was originally collected. Since this amounts to an authorisation to use the data for new purposes, it is subject to the constitutional requirements that apply to the further use of data for changed purposes as formulated in the Court's judgment on the Federal Criminal Police Office Act (cf. BVerfGE 141, 220 <326 ff. para. 284 ff.> with further references).

61 The authorisation to use data for new purposes constitutes a separate interference with the fundamental rights affected by the original data collection. For that reason, changes in purpose must be measured against the fundamental rights affected by the data collection. The weight attached to any such change in purpose in the balancing of interests is determined by the severity of interference associated with the data collection. Information obtained from measures constituting particularly intrusive interferences may only be used for particularly weighty purposes. In such cases, the principle of a hypothetical recollection of the data is the applicable standard for the proportionality assessment.

According to this principle, the decisive question for data obtained from intrusive surveillance and investigation measures is whether it would hypothetically be permissible, under constitutional law, to collect the relevant data again for the changed purpose using comparably intrusive methods. Thus, a change in purpose requires that the new use of the data serves to protect legal interests or detect criminal offences of such weight that it would, by constitutional standards, be justified to collect the data again using comparably intrusive methods as the original data collection. Yet in terms of the degree of specificity required for establishing the existence of a danger or the suspicion of criminal conduct, i.e. in terms of the threshold for interference, the requirements applicable to a change in purpose are not always the same as the requirements applicable to the original data collection. Under the principle of proportionality, these requirements primarily establish the direct grounds for the original data collection but not the grounds for further use of the collected data. An authorisation to use data for a new purpose constitutes a separate interference that requires new justification. For that reason, such an authorisation requires its own, sufficiently specific grounds prompting the measure. Under constitutional law, it is necessary, but generally also sufficient, that the data – either by itself or in combination with other information available to the authority – provides a specific basis for further investigations. 62

With regard to the use of the data by security authorities, the legislator may in principle allow a change in purpose if the data concerns information that, in the individual case, provides a specific basis for further investigations aimed at detecting comparably serious criminal offences or averting impending dangers that, at least in the medium term, threaten weighty legal interests that are comparable to the legal interests whose protection justified the original collection of the data. 63

But as with the further processing of data for purposes in line with the original purpose, this does not apply to information obtained from the surveillance of private homes or from covert access to IT systems. In view of the particular severity of interference resulting from these measures, each new use of such data is subject to the same justification requirements as the original data collection in that the new use also requires an acute danger or at least a sufficiently identifiable danger in the individual case. 64

c) Under § 25a of the Hesse Act and § 49 of the Hamburg Act, personal data may be subjected to further processing in line with the original purpose as well as further processing with a change in purpose. Both provisions allow for the processing of large amounts of data, essentially without differentiation as to the source of the data or the original purpose of its collection. In order to ensure adherence to the constitutional requirements arising from the principle of purpose limitation, other sufficiently clear provisions would therefore be required to achieve compliance with the principle of purpose limitation, both in legal terms and in practical application. When designing the statutory provisions to ensure compliance with the principle of purpose limitation, the legislator must furthermore take account of the fact that the automated analysis/interpretation of data which is currently stored in the authority's own IT system, but which was originally collected by another authority and then shared, cannot be regarded as further use with- 65

in the scope of the original purpose for collecting the data. Rather, it must be regarded as further use for a changed purpose – not least due to the change in the authority concerned – and is subject to the constitutional requirements that apply to the use of data for changed purposes. [...] In practical terms, this means that in order to comply with the constitutional principle of purpose limitation, the data must be labelled ([...]). However, whether these constitutional requirements were satisfied in the present case cannot be answered here because the issue was not admissibly challenged by the complainants (see para. 48 above).

2. With automated data analysis/interpretation, the severity of the original data collection is not the only factor to consider when assessing whether an interference with fundamental rights is constitutionally justified. This is because the use of automated data analysis/interpretation can result in new detrimental effects which might be more onerous than the severity of interference resulting from the original data collection (see a) below). The specific severity of interference resulting from automated data analysis/interpretation is not always the same, but rather depends on how the respective powers are designed. Using general standards, it is possible to determine which constitutional requirements apply to such powers (see b) below). The specific justification requirements then depend on how these powers are designed by the legislator in each case; here the justification requirements are strict due to the potential reach of § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act (see c) below). 66

a) If data that was already collected and stored at some earlier stage is further processed using automated data analysis/interpretation, this further processing can result in specific detrimental effects which might be more onerous than the severity of interference resulting from the original data collection (cf. BVerfGE 156, 11 <39 para. 73>). Automated data analysis/interpretation under § 25a of the Hesse Act and § 49 of the Hamburg Act is aimed at generating new intelligence. This process is described in § 25a(2) of the Hesse Act and § 49(2) of the Hamburg Act as the identification of connections between persons, groups of persons, institutions, organisations, objects and matters, the exclusion of insignificant information and intelligence, the matching of incoming information with known facts, and the statistical analysis of stored data. In legal terms, it allows the authorities involved to use practically any existing IT method to generate far-reaching intelligence from the available data and to deduce new connections by way of data analysis. Linking datasets makes it possible to perform multi-level analyses which can give rise to entirely new suspicions. It also provides a basis for performing further steps in the analysis process and subsequently instigating operational measures (BVerfGE 156, 11 <40 para. 73>). 67

In itself, there is nothing unusual about the police making further use of intelligence that was obtained at some earlier stage – either on its own or in conjunction with other available information – in order to provide leads for further lines of inquiry (cf. BVerfGE 141, 220 <325 f. para. 281>). Even the routine intelligence-gathering work carried out by the police involves linking and evaluating information obtained from different 68

sources ([...]).

Yet automated data analysis/interpretation pursuant to § 25a of the Hesse Act and § 49 of the Hamburg Act goes further than this because it enables large amounts of complex information to be processed. Depending on the analysis method used, the linking of existing datasets can generate new, otherwise inaccessible information that affects the personality rights of those affected. The measures in question thus intensify the generation of information from the data. Apart from extracting intelligence that was present in the data but had not yet been discovered because the datasets were not yet linked, this process can also come close to developing full profiles of the persons concerned ([...]). This is because the software can open up new possibilities of filling in the available information on a person by factoring in data and algorithmic assumptions about relationships and connections surrounding the person concerned. By combining personal and non-personal data, coupled where applicable with the fact that algorithms typically take into account mere correlations, new insights that would not otherwise be visible or detectable can be generated in ways that affect the personality rights of those concerned. The process vastly improves the effectiveness of conventional investigation methods, where authorities operate by gradually piecing together ever more information (cf. BVerfGE 115, 320 <356 f.> with further references – on electronic profiling). 69

In general, the principle of purpose limitation serves to ensure that interferences with fundamental rights resulting from the further processing of previously collected data are proportionate (see para. 55 ff. above). However, this principle was developed at a time when the task of reviewing and linking personal data was largely performed by humans, and when the amount of intelligence that could be generated was constrained by the practical limits on the amount of work that could be done. Yet the whole point of authorising the police to conduct automated data analysis/interpretation is to overcome these practical limits on the generation of intelligence. This is a legitimate aim under constitutional law because it increases the effectiveness of public security efforts. Nonetheless, one by-product of overcoming the practical limits of conventional police intelligence-generating activities is that persons affected by data processing are exposed to particular risks. Depending on how a given system is designed, especially in terms of the type and scope of usable data and the processing methods used, automated processing can make it possible to generate movement, behavioural and relationship profiles as well as more comprehensive personality profiles – profiles which could not be created through manual searches or rudimentary automated cross-checking. Automated data processing can thus bring major changes to the working methods and intelligence-generating capabilities of the police, thereby significantly increasing the severity of impairments of fundamental rights in individual cases (cf. also BVerfGE 156, 11 <39 f. para. 73> with further references). On its own, the constitutional principle of purpose limitation could then be inadequate in relation to the severity of interference. 70

b) The constitutional requirements for the justification of automated data analysis/interpretation vary (see aa) below), since one of the particular characteristics of data analysis/interpretation powers is that the severity of the resulting interference can differ 71

substantially depending on how these powers are designed in the legislation (see bb) below). The prerequisites for interfering with fundamental rights – in particular the threshold for interference, the legal interest to be protected and the necessary safeguards to ensure transparency, legal protection and administrative oversight (see cc) below) – vary accordingly and must be set forth in a way that satisfies the requirement that interferences be based on statutory provisions (*Gesetzesvorbehalt*) and that complies with the principles of legal clarity and specificity (see dd) below).

aa) The constitutional requirements for the justification of automated data analysis/interpretation vary, given that the severity of the resulting interference can differ substantially depending on how the relevant powers are designed in the legislation. If the powers only allow relatively small amounts of data from narrowly defined sources to be subjected to rudimentary cross-checking, the specific detrimental effects arising from data analysis/interpretation will be minor. But as the possibilities offered by automated data processing become increasingly powerful, the resulting interference becomes increasingly distinct from the original data collection and the principle of purpose limitation is less capable on its own of providing constitutional justification for this separate new interference. 72

If automated data analysis/interpretation gives rise to serious interferences with the informational self-determination of affected persons – for example by enabling the creation of precise movement, behavioural or relationship profiles, or by exposing persons who are not objectively involved in the relevant events to an increased risk of being specifically targeted by follow-up police investigations based on the results of the automated data analysis/interpretation – such interferences can only be justified subject to the strict requirements that apply to intrusive covert surveillance measures generally (see para. 104 ff. below). 73

If, on the other hand, the possibilities for obtaining intelligence are narrowed down to such a degree that no separate, particularly serious interference with the informational self-determination of affected persons can occur, the powers to use automated data analysis/interpretation can be linked to a lower threshold for interference, or the police can be permitted to exercise these powers for the protection of less weighty legal interests (see para. 107 below). Under certain circumstances, compliance with the principle of purpose limitation may be sufficient to provide constitutional justification for the further processing of data using automated methods (see para. 108 below for more details). 74

bb) With powers to conduct automated data analysis/interpretation, the stringency of the requirements applicable to the threshold for interference and the protected legal interests in each case is determined by the severity of the resulting interference, which depends on various factors and can be controlled by the legislator via different safeguards and combinations of protective mechanisms. 75

(1) In general, the severity of interference with informational self-determination primarily depends on the type, scope and possible uses of the data, as well as the risks of 76

abuse. In this regard, it is important how many holders of fundamental rights are exposed to impairments, how intense these impairments are, and on what basis they occur, in particular whether they were prompted by the persons concerned. The relevant criteria thus include the design of the statutory thresholds for interference, the number of persons affected, and also the severity of the individual impairments. The severity of individual impairments depends on whether the persons affected 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. Covert measures by the state result in interferences of greater severity, as do situations in which *ex ante* legal recourse is *de facto* denied and *ex post* legal recourse is difficult or even impossible to obtain (BVerfGE 156, 11 <48 f. para. 96> with further references; established case-law).

77 The specific severity of interference resulting from automated data analysis/interpretation largely depends on what type of new intelligence can be generated by the measures, in particular whether and to what extent they enable the generation of knowledge that affects the personality rights of the persons concerned. The severity of interference increases if the measures allow especially private information to be obtained. Measures are also particularly intrusive if they allow a person's behaviour, habits or lifestyle to be spatially reconstructed over a longer period of time, i.e. if they enable the creation of movement or relationship profiles as well as more comprehensive personality profiles (cf. BVerfGE 115, 320 <350 f.>; 120, 378 <400 f., 406 f., 417>; 125, 260 <319 f.>; 141, 220 <267 para. 99>; 150, 244 <284 f. para. 100>; Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 287, 321 ff.; Order of the First Senate of 9 December 2022 - 1 BvR 1345/21 -, para. 174 f. – *Police powers under the Security and Public Order Act for Mecklenburg-Western Pomerania*). Moreover, the severity of interference is greater if the police, having obtained information about persons through data analysis/interpretation, then use this information as the starting point for further operational measures even though the affected persons are not connected to any wrongdoing and did not prompt the police interference with conduct that can be attributed to them (cf. BVerfGE 115, 320 <354 f.>; 150, 244 <283 para. 98>), i.e. if the automated investigation methods used by the police increase the risk of objectively uninvolved persons being targeted by further police investigation measures (cf. BVerfGE 115, 320 <351 ff.>; 120, 378 <403>; 125, 260 <320>). In this respect, although the greater automation of police work does have the potential to prevent discrimination, it also harbours specific risks of amplifying discrimination. These risks become less tolerable under constitutional law, the more the effects of automated data analysis/interpretation are capable of producing disadvantages that are prohibited under Art. 3(3) of the Basic Law (cf. on electronic profiling BVerfGE 115, 320 <352 f.>; see also BVerfGE 154, 152 <259 para. 192>; [...]).

78 (2) The severity of interference primarily depends on the type and scope of the usable data. Electronic data processing's specific potential to interfere with fundamental rights is largely based on the amount of data that can be processed – an amount which could

in no way be handled by conventional means (cf. BVerfGE 156, 63 <118 f. para. 198> with further references). The greater the amount of personal data that can be included in automated data analysis/interpretation – i.e. the less the legislator restricts the amount of usable data –, the more serious the interference becomes. Rules on the amount of data that can be used are closely related to rules on the type of data that can be used. The less restrictions are placed on the type of data that can be used, the more data is available for processing and the more serious the interference tends to be. The type of data is also significant in its own right in determining the severity of interference because the use of different kinds of data can, either directly or indirectly, affect personality rights to varying degrees. The type and scope of usable data and the resulting impact on the severity of interference with fundamental rights can be specified in greater detail and limited by various safeguards.

(a) The severity of interference can be reduced by statutory provisions regarding the sources of the data. For example, processing can be limited to data originally collected by the authority itself or data originally collected by another authority within the same *Land*, or at least by another authority in Germany. Data obtained from social networks can be excluded. Processing can be limited to data originally collected by a police authority (within the *Land* concerned). Data originally collected by intelligence services can be excluded. 79

(b) The type and scope of usable data can also be limited by statutory provisions relating to the circumstances of the original data collection. In particular, the scope of the usable data can be restricted by purpose limitation rules (see para. 55 ff. above). If there are organisational or technical safeguards in place to ensure that data is only processed in accordance with its statutorily permitted use, and if the statutorily permitted use is defined in sufficiently narrow terms, the scope of data available for processing can be significantly reduced. Examples of technical and organisational safeguards designed to ensure compliance with purpose limitation requirements include the technical separation of datasets according to different processing purposes, and the granting of access rights to data depending on the purpose pursued ([...]). 80

The severity of interference can also be reduced by excluding data originally obtained from particularly serious interferences with fundamental rights (for an example, see § 6a(3) in conjunction with § 4 of the Counter-Terrorism Database Act, *Antiterrordateigesetz* – ATDG). That said, data obtained from the surveillance of private homes or remote searches may only be used under extremely strict conditions anyway if the analysis/interpretation is conducted as a precautionary measure for the prevention of criminal offences. Given the extraordinary severity of interference resulting from the surveillance of private homes and remote searches, it is only justifiable to process the obtained data if this is necessary to avert an acute danger or a sufficiently identifiable danger in the individual case (cf. BVerfGE 141, 220 <326 para. 283; 329 para. 291>). Due to the principle of purpose limitation, data obtained from other serious interferences may likewise only be used for the changed purpose of data analysis/interpretation conducted as a precautionary measure for the prevention of criminal offences if, in the individual case, the da- 81

ta provides a specific basis for further investigations aimed at averting impending dangers that may emerge at least in the medium term (cf. BVerfGE 141, 220 <329 para. 290>; see also para. 63 above).

In addition to setting purpose limitations, the legislator can impose source-related restrictions on the data by only permitting data from certain police activities to be used in automated data processing (cf. for example § 2 first sentence, first half-sentence of the Counter-Terrorism Database Act – only data from counter-terrorism measures). 82

(c) The amount of usable data can also be limited by narrowing down the criminal offences whose prevention would justify the precautionary use of automated data analysis/interpretation, in that data may only be used if its inclusion is necessary to prevent these more precisely defined criminal offences (cf. for example § 2 first sentence of the Counter-Terrorism Database Act). 83

(d) The severity of interference can furthermore be reduced if use is only made of data that relates to persons who, based on factual indications known to the police, are suspected of being involved in (sufficiently weighty) criminal offences or of being in close contact with such persons (cf., e.g., § 2 and § 3(2) of the Counter-Terrorism Database Act). Limitations of this type would reduce the risk of obtaining information on persons who have not provided any attributable grounds for suspicion themselves but could nevertheless be exposed to operational follow-up measures by the police. 84

(e) The amount of usable data is also determined by statutory provisions relating to retention periods and deletion requirements. If traffic data – in particular data obtained from radio cell queries (cf., e.g., § 100g(3) Code of Criminal Procedure) – is included within the data pool available for automated data analysis/interpretation and if large amounts of such data can be retained, substantial restrictions must be imposed on the amount of collectable data and a maximum retention period must be set (cf. BVerfGE 154, 152 <259 para. 191> for the powers of the intelligence services to conduct surveillance of foreign telecommunications). 85

On the other hand, even though data analysis/interpretation makes use of vast quantities of data relating to a large number of persons, the overwhelming majority of whom have no involvement in the events in question, the severity of interference is reduced by the fact that the data matching process is completed in a matter of seconds and, in the case of non-matches, the collected data gives rise to no further police action (cf. BVerfGE 150, 244 <283 para. 97>). 86

(f) Depending on their content, provisions governing the permitted types of data (cf. e.g. § 3(1) of the Counter-Terrorism Database Act) can also serve to limit the amount of usable data. This includes provisions that specify the file formats that are usable in data analysis/interpretation (e.g. photographs, video, audio recordings). For instance, the exclusion of biometric data can reduce the severity of interference. 87

(g) In practice, the amount of usable data can also be reduced if the statutory framework specifies that files may not be included automatically but must be added manually 88

for each data analysis/interpretation measure. Conversely, if the data analysis/interpretation platform is connected to the internet, this increases the severity of interference because it facilitates the processing of especially large amounts of data.

(h) Technical and organisational safeguards can also be used to reduce the amount of personal data that is usable in data analysis/interpretation by only granting access rights to a limited number of staff members who must satisfy particular criteria. If only a small number of persons have access to the analysis platform and access is only granted for precisely defined purposes, data analysis/interpretation measures are likely to be carried out less frequently and less data will be processed. 89

(3) The severity of interference is also influenced by the permitted methods of data analysis/interpretation. The use of complex forms of data matching can result in interference of a particularly serious nature. If the police can make use of practically any existing IT method to extract far-reaching intelligence from the available data, allowing them to identify new connections, generate new suspicions from multi-level analyses, and follow up by carrying out further steps in the analysis process or by instigating operational measures, the impact of automated data analysis/interpretation on the persons concerned can be extremely adverse and the severity of the individual impairment can be significantly increased (cf. BVerfGE 156, 11 <39 f. para. 73> with further references). Furthermore, with complex forms of data matching, the algorithms involved can be difficult to scrutinise. This has implications for individual legal protection and administrative oversight, both of which are rendered impossible without the ability to identify and rectify errors (cf. BVerfGE 154, 152 <259 f. para. 192>). In general, the severity of interference resulting from the permitted methods of automated data analysis/interpretation depends on the breadth and depth of the personal information that can be generated, the extent of the margin of error, the likelihood of discrimination, and the difficulty of scrutinising the connections made by the software. 90

(a) The severity of interference resulting from automated data analysis/interpretation tends to decrease, the more the process resembles a rudimentary cross-checking operation. With rudimentary cross-checking, the existing data on a person is located by entering the person's details into the particular system and running those details past the stored data. When conducted as an automatic process, cross-checking often brings datasets together in order to identify correlations in the data or transfer data from one dataset to another ([...]). Rudimentary cross-checking thus involves a search-based comparison of data in order to identify matches ([...]). 91

Nevertheless, search-based cross-checking can become more complex if the number of steps in the matching process and the number of links between datasets increase. But if, from the outset, there is a limit on the number of pre-programmed matching steps that can be performed without being prompted by further human intervention in the individual case, the possibilities for linking data are reduced, thereby helping to lessen the severity of interference. 92

(b) By contrast, the severity of interference becomes greater, the more openly the 93

search process is structured and the less that automated data analysis/interpretation is guided by the parameters of conventional police search profiles, which are typically enhanced by insights and assumptions relating to the specific case. This is because when an automated search is conducted as a precautionary measure for the prevention of criminal offences in situations where no specific danger has yet arisen, the search is more likely to detect indications of danger, the more openly the process is structured (i.e. the less the search is based on the facts of any specific case). In particular, the interference becomes more serious when data analysis/interpretation is not based on a particular search term, at least not on a search term related to already known facts, but where the analysis/interpretation process is aimed entirely at identifying distinctive statistical features in the available data – distinctive features which, in additional steps, are (automatically) linked with information in other datasets and can then give rise to further intelligence that the police did not previously have any grounds to search for.

The interference also becomes more serious when search queries are not directed at specifically defined persons and when no factual connections are required between the legal interest under threat and the persons affected by automated data processing. Such cases then lack any facts-based connection between a particular danger and a person specifically responsible for causing that danger. Indeed, the relevant connections are only established during the data processing stage itself, and there is an increased risk of persons being included in further police measures despite not having provided any grounds for suspicion through actions that are attributable to them (cf. also BVerfGE 115, 320 <361 f.>; Federal Constitutional Court, Order of the First Senate of 9 December 2022 - 1 BvR 1345/21 -, para. 189 – on electronic profiling). 94

The risks associated with openly structured searches can be reduced by establishing a strict threshold for exercising the relevant powers (see para. 104 ff. below) and can also be lessened by imposing limits on the permissible methods of data processing. In order to do this, the statutory framework must restrict the search process in a way that requires the search to be based on relatively specific grounds. If the legislator places less demanding requirements on the permissible grounds for data analysis/interpretation, it must impose more precise and narrowly-defined requirements on the permissible search methods. Under constitutional law, it is not permissible for large amounts of personal data to be subjected to automated data processing in order to search for previously undetected patterns and correlations of public security significance, unless this process is based on specific grounds in the individual case or is limited by rules governing the permissible processing methods. If a statutorily permitted method allows large amounts of data to be processed, and especially if the intention is to thereby enable the detection of statistical correlations, then sufficient data quality must be ensured and safeguards must be in place to prevent the selection of data from having any inappropriately distorting or discriminatory effects (see para. 77 above). 95

(c) The severity of interference also depends on what kind of search results are generated by automated data analysis/interpretation. 96

For example, if data analysis/interpretation is merely aimed at identifying dangerous or sensitive locations rather than at obtaining intelligence on specific persons, the interference is generally less serious. 97

If, on the other hand, automated data processing is used to generate intelligence on specific persons and this information contains machine-driven evaluations that go beyond the simple detection of matches between the search criteria and the searched data, the interference is particularly serious. Where the level of danger posed by a specific individual is machine-evaluated in the manner of 'predictive policing', this has a particularly exacerbating effect on the severity of interference ([...]). 98

(d) However, the severity of interference with informational self-determination resulting from the use of automated data analysis to generate new intelligence can be reduced by tying the use of this new intelligence to specific conditions. This is because the severity of interference with informational self-determination is also generally influenced by the way in which the obtained personal information is used and the consequences this can have for the persons concerned (cf. Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 157 with further references; established case-law). 99

(e) The use of self-learning systems – i.e. artificial intelligence or AI – can interfere with fundamental rights in a particularly intrusive manner depending on the particular use in question. The advantages of such systems – as well as the specific dangers they pose – lie in the fact that they do not simply apply the criminologically sound profiles used by individual police officers, but rather that they automatically refine these profiles, or in some cases even create entirely new ones, and then continue to combine them during further stages of the analysis. Using complex algorithms, automated data processing software is thus capable of going beyond the mere identification of relationships and connections, and can begin autonomously producing further evaluations in the manner of 'predictive policing'. This enables particularly far-reaching insights and assumptions to be generated about a person. The verification of such information can be difficult in practice because, over the course of the machine learning process, complex algorithmic systems can increasingly detach themselves from the human programming that created them, with the machine learning process and the results generated becoming increasingly difficult to scrutinise (cf. CJEU, Judgment of 21 June 2021, *Ligue des droits humains*, C-817/19, ECLI:EU:C:2022:491, para. 195). State oversight over the technology could then be rendered impossible. Furthermore, if software from private actors or foreign states is deployed, there is a risk that third parties could manipulate or gain access to data in undetected ways ([...]). Another specific challenge is to prevent the emergence and application of algorithmic discrimination. Self-learning systems may only be used in police work if special procedural safeguards are in place to ensure that sufficient levels of protection are guaranteed despite the reduced possibilities for exercising scrutiny. 100

Even with deterministic systems whose analytical functions are not capable of evolving independently but are rigidly programmed into the software, the analytical process can 101

be complex and largely beyond scrutiny for users and affected persons alike. If the legislator wishes to permit intrusive methods of data analysis – complex forms of data matching in particular –, then it must ensure that a protective legal framework is in place (cf. BVerfGE 154, 152 <259 f. para. 192>).

(f) Overall, the severity of interference resulting from automated data analysis/interpretation also depends on how error-prone the data analysis technology is and whether safeguards are in place for identifying and rectifying errors. 102

cc) The constitutional requirements applicable to the prerequisites for interference correspond with the severity of interference resulting from automated data analysis/interpretation, which the legislator can control by setting out rules on the type and scope of usable data and by limiting the permissible methods of analysis. Thus, the question of whether a statutory provision authorising automated data analysis/interpretation satisfies the constitutional requirements is partly dependent on whether the legislator has established prerequisites for interference that are sufficient in view of the specific design of the powers. For any given measure, the requirements arising from the principle of proportionality in the strict sense correspond to the severity of interference; they apply to both the legal interest to be protected and the threshold for interference, i.e. the grounds for carrying out the measure (cf. also BVerfGE 141, 220 <269 para. 104, 270 f. para. 106 ff., 271 ff. para. 109 ff.>; Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 174; Order of the First Senate of 9 December 2022 - 1 BvR 1345/21 -, para. 89; see para. 104 ff. below). As explained above (see para. 75 ff.), the legislator has at its disposal a variety of options to control the severity of interference with informational self-determination resulting from automated data analysis/interpretation so as to ensure that the severity is proportionate to the respective threshold for interference and to the weight of the public security interests involved (cf. also BVerfGE 115, 320 <360>). If automated methods give rise to separate and serious interferences with the informational self-determination of affected persons, such interferences may only be justified subject to strict requirements (see (1) below). Less serious interferences may be justifiable on less weighty grounds (see (2) below). Under certain circumstances, compliance with the principle of purpose limitation may be sufficient (see (3) below). In any event, the principle of proportionality gives rise to requirements regarding transparency, individual legal protection and administrative oversight (see (4) below). 103

(1) If, based on the aforementioned criteria, automated methods give rise to serious interferences with the informational self-determination of affected persons, such interferences may only be justified subject to the strict requirements that apply to intrusive covert surveillance measures generally. 104

(a) Demanding requirements must then be imposed on the legal interest to be protected by automated data analysis/interpretation. Covert surveillance measures that reach deep into a person's private life are only permissible to protect particularly weighty legal interests (BVerfGE 141, 220 <270 para. 108>). Particularly weighty legal interests in 105

this sense include life, limb and liberty of the person, as well as the existence or security of the Federation or a *Land* (cf. BVerfGE 133, 277 <365 para. 203>; 141, 220 <270 f. para. 108, 328 ff. para. 288, 292>; 154, 152 <269 para. 221>; 156, 11 <55 para. 116>; Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 243). One comparably weighty legal interest is the protection of assets of substantial value, the preservation of which is of public interest, insofar as this is narrowly interpreted as meaning significant infrastructure facilities or other sites that are vital for society (cf. Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 244, with reference to BVerfGE 141, 220 <296 para. 183> and BVerfGE 133, 277 <365 para. 203>). If it so wishes, however, the legislator may refrain from specifically naming the required legal interest and can instead make reference to the criminal offences that the powers in question must serve to prevent (cf. BVerfGE 154, 152 <269 para. 221>; Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 244).

(b) Strict limits must then also be placed on the permissible grounds for interference. Like with most covert surveillance measures carried out by public security authorities and involving deep intrusions into the private sphere, the constitutionally required threshold for interference here is the existence of a sufficiently identifiable danger (for specific details, BVerfGE 141, 220 <272 f. para. 112>). This is the generally applicable threshold for the use of covert surveillance measures by public security authorities (cf. Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 248 with further references). In order for a sufficiently identifiable danger to be present, there must be at least factual indications that a specific danger to the protected legal interests may emerge. Assumptions based on general experience alone are not sufficient. Rather, specific facts must be established that, in the individual case, support the prognosis that a chain of events leading to a violation of one of the protected legal interests will occur and that the violation can be attributed to the person against whom the measure is directed. A sufficiently identifiable danger in this sense may already exist even where the causal chain leading to the damage is not yet foreseeable with sufficient probability, provided that there are already specific facts indicating an impending danger to an exceptionally significant legal interest in the individual case. 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 measure can be targeted at them and for the most part limited to them (BVerfGE 141, 220 <272 para. 112>). 106

(2) Provided that an identifiable danger exists, less serious interferences may be justified if they serve to protect legal interests of at least considerable weight, as is the case with the prevention of criminal offences that are at least considerable. In turn, a threshold below the level of an identifiable danger may be sufficient if a measure serves to protect high-ranking, exceptionally significant or particularly weighty legal interests (cf. BVerfGE 155, 119 <188 f. para. 150> with further references). Thus, measures that give 107

rise to serious interference require the existence of an identifiable danger in combination with the purpose of protecting particularly weighty legal interests, whereas for less serious measures it is sufficient if the statutory provision authorising the interference requires either an identifiable danger or the purpose of protecting particularly weighty legal interests (cf. Federal Constitutional Court, Order of the First Senate of 9 December 2022 - 1 BvR 1345/21 -, para. 173). This is particularly relevant if the legislator reduces the severity of data analysis/interpretation by imposing stricter rules on the type and scope of usable data and the permissible data processing methods.

(3) If the type and scope of usable data are limited by statutory provisions, and the permissible methods of analysis/interpretation are restricted to such a degree that a measure carried out on the basis of the power in question will not lead to more extensive insights into the life of affected persons than what could realistically be obtained by the authority, albeit more slowly and laboriously, without automation, or if the power is purely aimed from the outset at identifying dangerous or sensitive locations without generating personal information, then adherence to the principle of purpose limitation alone may be sufficient for justifying the further processing of the data by automated methods (see para. 55 above). However, it would be impermissible under constitutional law for police authorities, without any grounds whatsoever, to subject personal data to automated analysis conducted as a precautionary measure for the prevention of criminal offences. That said, adherence to the principle of purpose limitation would ensure that grounds for such interference do exist. 108

(4) In any case, the principle of proportionality gives rise to requirements regarding transparency, individual legal protection and administrative oversight (cf. BVerfGE 141, 220 <282 para. 134> with further references; established case-law). In particular, it is important that the oversight system is properly designed. Given the potentially large number of measures involved, the task can be divided between independent data protection officers and data protection officers working within a given authority based on a graduated oversight system. The oversight process can also be structured in the form of random checks. In order for oversight to be effective, it is essential that written justifications are given in each individual case as to why certain datasets are subjected to automated data analysis for the purpose of preventing certain criminal offences. If software is deployed that enables more complex forms of automated data matching, safeguards are necessary to address the high error rates specifically associated with such processes. This may require the introduction of statutory provisions to ensure state monitoring of the software's performance over time. What specific requirements need to be imposed on such additional safeguards is not the subject of the current proceedings. 109

dd) The threshold of an at least identifiable danger to particularly weighty legal interests can only be constitutionally dispensed with if the legal framework, in a clear and sufficiently specific manner, limits the permissible methods of analysis/interpretation so narrowly that the severity of interference resulting from the measures is substantially reduced. In principle, the legislator may divide the task of setting out such rules, laying down some elements itself while allowing other rules to be determined by the admin- 110

istrative authorities (see (1) below). However, the legislator must ensure that the rules – in particular those limiting the type and scope of usable data (see (2) below) and restricting the permissible methods of data processing (see (3) below) – are sufficient as a whole and adhere to the requirement that interferences be based on statutory provisions.

Whether the legislator is still obliged to enact rules limiting the type and scope of usable data and restricting the permissible methods of data processing even if it ties the power to conduct data analysis/interpretation to the strict threshold of an at least identifiable danger to particularly weighty legal interests is not an issue that must be addressed here. Likewise, there is no need to examine whether the constitutional purpose limitation requirements for data analysis/interpretation have been sufficiently set out in the statutory framework and whether there are sufficient rules on transparency, individual legal protection and administrative oversight (see para. 48 above). In this respect, the question of compatibility with the requirement that interferences be based on statutory provisions does not arise. 111

(1) If, like here, the legislator wishes to authorise the police to conduct automated data analysis/interpretation as a precautionary measure for the prevention of criminal offences, i.e. before any identifiable danger has arisen, it must reduce the severity of the resulting interference in order to ensure proportionality. With the existing options for doing this, namely limiting the type and scope of usable data and restricting the permissible methods of data processing, the legislator must adhere to the requirement that interferences be based on statutory provisions. The legislator itself must provide for the basic legal framework limiting the type and scope of usable data and the permissible data processing methods. Since the rules needed here to lessen the severity of interference are of a particularly technical nature and require frequent updating, the legislator may authorise the administrative authorities to issue detailed organisational and technical rules in cases where addressing the subject matter in depth with parliamentary legislation does not appear practicable. The legislator must however ensure that, taken as a whole, the statutory requirements in conjunction with the powers and obligations conferred upon the administrative authorities to issue further rules serve to limit the type and scope of usable data and the permissible methods of data processing in a sufficiently precise, clear and transparent manner. 112

For the determination of aspects that do not have to be set out by the legislator, a statute authorising the administrative authorities to issue ordinances may be considered. The legislator may also oblige the administrative authorities to further specify the abstract and generalised requirements contained in legislation or ordinances. That said, specification by way of administrative rules requires a statutory basis. In this statutory basis, the legislator must ensure that the authorities comprehensibly document and publish the specifying and standardising determinations that will ultimately govern the application of the provisions in the individual case (cf. also BVerfGE 133, 277 <357 para. 183>). If the requirements regarding the type and scope of usable data and the permissible methods of data processing are only partly discernible from the legislation itself, 113

these requirements must be specified and standardised in a comprehensible manner by the administrative authorities. As a compensatory safeguard, it is then necessary to impose special transparency requirements on the administrative authorities because the persons affected by automated data analysis/interpretation are not usually aware that such measures have been carried out, making it virtually impossible for the relevant statutory provisions to be refined through the interplay between administrative action and judicial review. The absence of review by the administrative courts means that a central mechanism for reviewing power-granting provisions that require further specification is largely missing. In order to compensate for this anomaly, the legislator must ensure that the administrative authorities lay down the requirements and criteria that apply to automated data analysis/interpretation in the individual case in an abstract and generalised manner, that they ensure reliable documentation, and that they publish their determinations in a form to be specified by the legislator. On the one hand, this system of determination, documentation and disclosure serves to keep the powers granted to the administrative authorities in check. On the other hand, it ensures that oversight can be properly exercised, because requiring the administrative authorities to document and disclose their criteria provides data protection officers, in particular, with the means to review the executive's exercise of powers (cf. BVerfGE 133, 277 <357 f. para. 184> with further references).

Insofar as the legislator is obliged to lay down certain aspects itself, it must do so in a sufficiently specific and clear manner (cf. BVerfGE 156, 11 <45 f. para. 86 f.>). Insofar as requirements regarding the limitation of data processing are already contained in the provisions of general data protection law and police data protection law, the fact that these provisions apply to the powers of data analysis/interpretation must be sufficiently recognisable both for the authority in question and for the general public. Likewise, it must be sufficiently clear what the resulting implications are for the practical design of these powers. 114

(2) If the legislator wishes to reduce the severity of interference so that the instrument of automated data analysis/interpretation can be used even before any identifiable danger has arisen, it must set out the basic rules concerning the type and scope of the usable data itself. 115

In particular, the datasets that may be integrated into the analysis platform and the extent to which this may be done automatically must be specified in the legislation itself. If the legislator does not provide an exhaustive list of the usable datasets itself, it must ensure that abstract and generalised criteria are provided for and published in delegated legislation. The class of datasets that may be (automatically) integrated is not rigidly defined under constitutional law. That said, the greater the size and number of datasets that can be used, the greater the severity of interference (see para. 78 ff. above); stricter requirements must then be applied to the permissible grounds for interference and the legal interest to be protected. 116

Unless the usable datasets are subject to highly restrictive substantive and quantitative 117

limitations from the outset, the legislator must furthermore limit the automated data analysis/interpretation process by ensuring that access to the platform is only granted to specific, appropriately qualified police officers and that these persons can only use the platform in accordance with the grounds for interference to be specified in the legislation. These access limitations must be implemented not only in the form of legal restrictions but also through organisational and technical safeguards. Technical details may be specified in the rules to be published by the administrative authorities.

118 In order to comply with the constitutional principle of purpose limitation (see para. 55 ff. above), the legislation itself must include the requirement that data obtained from the surveillance of private homes or remote searches may not be used in data analysis/interpretation conducted as a precautionary measure for the prevention of criminal offences (see para. 59 and 64 above). Insofar as data is obtained from other serious interferences with fundamental rights, the further use of such data may only be permitted in cases where it contains information that, in the individual case, provides a specific basis for further investigations aimed at averting impending dangers that threaten comparably weighty legal interests at least in the medium term (see para. 63 above). Here too, the legislator must lay down the necessary rules itself. In both constellations, the legislator must also lay down rules to ensure that the limitations are effectively implemented by appropriate technical and organisational safeguards that take account of the special characteristics of automated data analysis/interpretation, especially where the automated integration of data is concerned. In particular, information obtained from data collection methods that seriously interfere with fundamental rights must be labelled or separated prior to data analysis/interpretation so that access to such information can be prevented where necessary. It is not permissible to delay identifying the source of such information until after data analysis/interpretation has been carried out, as the representative of the complainants in proceedings 1 BvR 1547/19 feared might happen (see also para. 144 below). The legislator may leave the task of specifying the appropriate protective requirements to the administrative authorities. However, the administrative authorities must clearly formulate these requirements in abstract and generalised terms and must publish them. Unless practical measures are in place to ensure that data obtained from particularly serious interferences with fundamental rights can only be used in automated data analysis/interpretation under the aforementioned conditions, the powers may not be exercised to conduct precautionary measures for the prevention of criminal offences.

119 There are additional possibilities for reducing the severity of interference by restricting the type and scope of data that can be used in automated data analysis/interpretation (see para. 78 ff. above). But here too, the requirement that interferences be based on statutory provisions is applicable. This means that further restrictions only serve to lower the constitutional requirements that apply to the statutory thresholds for interference and the legal interest to be protected if the essential aspects of these restrictions are set out in the legislation itself, or if the legislation delegates the power to issue such restrictions to the administrative authorities who then clearly formulate, document and pub-

lish such restrictions in abstract and generalised terms.

(3) If the legislator wishes to reduce the severity of interference so that automated data analysis/interpretation can be used even before any identifiable danger has arisen, it must furthermore restrict the permissible methods of automated data analysis/interpretation and set out the basic permissible characteristics of such processing in the legislation itself. 120

The use of self-learning systems must be explicitly ruled out in the legislation. In addition, the legislator itself must lay down basic rules to limit the degree of automation. It is not sufficient for the police authorities to merely set up the data analysis/interpretation platform in a way that prevents it going beyond rudimentary automated cross-checking or that prevents the matching process being automatically repeated so as to match the results with other datasets. Rather, restrictions on the permissible methods of data matching must be contained in the legislation itself. If the legislator wishes to reduce the severity of interference by requiring that the search process be limited to individual search terms that comply with the parameters of conventional police search profiles, thereby preventing the search process from being entirely open (see para. 93 ff. above), it would have to create the necessary legal framework itself, at least the basic aspects thereof. If it wishes to reduce the severity of interference by limiting the possible results of the analysis, it would also have to at least specify some basic rules (see para. 96 ff. above). For example, if the legislator wishes to exclude machine-driven evaluations that go beyond the simple detection of matches between the search criteria and the searched data, particularly if the legislator wishes to exclude machine-driven evaluations that assess the level of danger posed by specific individuals in the manner of 'predictive policing', or if the legislator's aim from the outset is to direct data analysis/interpretation solely at identifying dangerous or sensitive locations, then the legislator itself must explicitly specify this in order for the severity of interference to be reduced. However, the task of designing the analysis process in more detail can be left to the administrative authorities (cf. also BVerfGE 154, 152 <259 para. 192>), which would then have to formulate the requirements in abstract and generalised terms and would have to publish them. 121

There are further possibilities for reducing the severity of interference of automated data analysis/interpretation by restricting the permissible methods of data processing (see para. 90 ff. above), but these restrictions only lower the constitutional requirements that apply to the statutory thresholds for interference and the legal interest to be protected if they satisfy the requirement that interferences be based on statutory provisions and if additional rules are clearly formulated, documented and published in abstract and generalised terms by the administrative authorities. 122

c) Based on the general standards set out above, the provisions authorising the police to conduct data analysis/interpretation under § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act – which are broadly worded in terms of the usable data and the permissible methods – can potentially give rise to interferences 123

of a very serious nature (see aa) below). Constitutional law therefore requires that these provisions meet strict prerequisites for interference (see bb) below).

aa) Given the type and scope of data that can be used (see (1) below) and the permissible methods of data processing (see (2) below), the challenged data analysis/interpretation powers can potentially give rise to interferences of a very serious nature. 124

(1) Both provisions impose almost no restrictions on the type and amount of data that can be used for data analysis/interpretation. They do not specify what types of data or what datasets may be used for automated analysis/interpretation. 125

(a) The provisions do not differentiate between persons who provide grounds for the suspicion that they might commit a criminal offence or have some particular connection to such persons (cf. § 2 of the Counter-Terrorism Database Act) and persons who provide no such grounds. This is relevant because the inclusion of data from case management systems (see para. 133 ff. below) and radio cell queries (see para. 142 below) means that large amounts of personal data are channelled into data analysis/interpretation despite the persons affected not having provided the police with any grounds to conduct precautionary measures for the prevention of serious criminal offences. Law enforcement datasets can also contain information of this nature, e.g. data on victims or witnesses. Furthermore, persons who in the past were responsible for criminal activity or for causing danger (within the meaning of police law) and whose data may be further processed under § 20(6) and (7) of the Hesse Act and § 36(2) and (3) of the Hamburg Act often bear no such responsibility in the present. Their data is nonetheless included in the analysis because the provisions do not require an unfavourable prognosis in order for their data to be used ([...]). Overall, the provisions allow the extensive inclusion of data relating to innocent third parties ([...]), with the result that such persons could be subjected to further police investigations despite not having provided any attributable grounds for suspicion. 126

(b) The provisions do not specify what datasets may be included. While § 49 of the Hamburg Act – unlike § 25a of the Hesse Act – does limit the scope of data processing to data stored in police filing systems, this does not require that the data was originally collected by the police, nor does it place any source-based restrictions on what stored data may be used. For example, it does not exclude data from other *Länder*, from the Federation's area of responsibility or from foreign countries. Nor does it exclude data from other non-police authorities or even from non-public entities. Nor do the provisions expressly prohibit the further use of data collected by intelligence services for the purpose of averting an at least identifiable danger (cf. BVerfGE 156, 11 <55 para. 118>; Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 245; Order of the First Senate of 28 September 2022 - 1 BvR 2354/13 -, para. 132 ff. - Federal Protection of the Constitution Act - data sharing powers). 127

The question of whether datasets may be integrated automatically into the data analysis/interpretation process is not specifically addressed either. 128

Nor does the term 'filing system', which appears in § 49 of the Hamburg Act but not in § 25a of the Hesse Act, serve to narrow down the usable data. According to § 2(13) of the Hamburg Act, a 'filing system' is any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or categorised according to functional or geographical criteria. The type, number and content of such police filing systems are not prescribed by law. Moreover, the term 'filing system' encompasses more than the automated databases operated by the police system in question. In any case, it is possible to create new filing systems, including at short notice if necessary. 129

(c) Insofar as general rules governing the further use of data are contained in other legislation, these could potentially serve to exclude certain data and datasets from data analysis/interpretation. But in order to reduce the severity of interference resulting from measures conducted under § 25a of the Hesse Act or § 49 of the Hamburg Act in a constitutionally significant manner, there would need to be greater precision in specifying how these rules apply in both legal and practical terms to automated data analysis/interpretation. The challenged provisions do not contain anything to this effect. In particular, there is no specification of the necessary organisational and technical safeguards. 130

(aa) In principle, general rules on the further use of previously collected and stored data could serve to limit the type and amount of data that can be used in data analysis/interpretation and could thus reduce the severity of interference. In particular, the police in Hesse and Hamburg are restricted in the further processing of data by the general principle of purpose limitation in § 20 of the Hesse Act and § 34 of the Hamburg Act. Yet as the current proceedings have shown, there is uncertainty surrounding the extent to which the general purpose limitation rules in § 20 of the Hesse Act and § 34 of the Hamburg Act apply to automated data analysis/interpretation. In any case, these rules are not specific or clear enough to lessen the severity of interference, while practical reasons prevent them from having any limiting effect on their own. 131

(α) For example, as the legal representative for the Free and Hanseatic City of Hamburg explained at the oral hearing, § 49 of the Hamburg Act could be understood as offering exemption from the principle of purpose limitation from the outset. Given the practical difficulties of ensuring that every piece of data complies with purpose limitation requirements when dealing with software that is specifically designed to merge different pieces of data into a single pool using automated processes, this is not an unreasonable interpretation of ordinary law. 132

(β) In Hessian law, there is uncertainty as to whether § 20(9) third sentence of the Hesse Act is to be understood as meaning that the general purpose limitation rules in § 20(1) and (2) of the Hesse Act do not apply to the large amount of case management data and its inclusion in automated data analysis under § 25a of the Hesse Act, or whether the general rules in § 20(1) and (2) of the Hesse Act do in fact apply and, if so, whether they have any significant impact on limiting the amount of data. 133

The volume of data used in data analysis is significantly increased by the inclusion of case management data. In this context, a 'case' encompasses all the records kept in con- 134

nection with police activities relating to a certain person, object or other subject matter of police action ([...]). The police make use of case management systems to record the data they need to carry out their specific tasks in individual cases. Among the main categories of items stored are complaints, investigation reports and memos – including on traffic accidents. The systems also contain data on the persons who file complaints or provide information, as well as data on witnesses, persons involved in accidents, and other persons who are not suspects or accused persons within the meaning of criminal procedural law and who are not responsible for causing danger within the meaning of police law ([...]). In Hesse, this data is automatically integrated into the analysis platform ([...]).

Whether the restrictions of § 20(1) and (2) of the Hesse Act apply to the inclusion of case management data in automated data analysis is therefore of major significance in determining the scope of data processing. Yet this question is neither clearly addressed in the legislation, nor is it clarified in practice. In their written statements, both the Hessian Officer for Data Protection and Freedom of Information and the Federal Officer for Data Protection and Freedom of Information assumed that the restrictions did not apply to case management data. The wording of § 20(9) of the Hesse Act would suggest that this is an entirely reasonable explanation, especially since the legislator's intention was to use automated analysis to overcome the existing barriers between the various datasets ([...]). But at the oral hearing, the Hessian Ministry of the Interior and Sports and the Hessian Officer for Data Protection and Freedom of Information both agreed that the general principle of purpose limitation was nonetheless applicable. The issue is not clearly dealt with in § 20(9) of the Hesse Act. 135

Be that as it may, a pragmatic interpretation of the meaning of § 20(2) first sentence no. 2 of the Hesse Act when applying § 25a of the Hesse Act suggests that the amount of usable data would not be significantly reduced even if the restrictions did apply. At the oral hearing, the Hessian Ministry of the Interior and Sports responded to the question of how one could ensure that a given piece of data in the case management system provided a specific basis for further investigations – as required under § 20(2) first sentence no. 2 of the Hesse Act – by stating that from a criminological perspective, one could never rule out the possibility of data being significant for the prevention of the type of criminal offences that data analysis is aimed at preventing. As to the quantitative significance of case management data for data analysis, the Ministry described it as extremely important; nobody who featured in the data was 'uninvolved' in the police sense because as soon as anything related to a person was documented in the case management system, that person was 'involved'. It is not therefore evident that the volume of data obtained from the case management system would actually be reduced to a minimal amount even if § 20(2) first sentence no. 2 of the Hesse Act did apply to data analysis (but see para. 159 ff. below regarding further practical restrictions in Hesse based on the criterion of an 'individual case'). 136

Overall, the general rules on purpose limitation do not restrict the scope of usable data with sufficient clarity to significantly reduce the severity of interference of data analysis/ 137

interpretation under constitutional law.

(?) In cases where large datasets are processed using automated data analysis/interpretation and some of that data is integrated into the platform automatically, practical constraints prevent the purpose limitation requirements from limiting the amount of usable data on their own, because the sheer amount of data involved combined with the fact that some of the data is automatically integrated into the platform make it difficult to identify and check the purpose of each individual piece of data. 138

Even though labelling requirements do exist (cf. § 20a of the Hesse Act, § 65 of the Hamburg Act), broad use is made of the available exemptions (cf. § 20a(4) of the Hesse Act, § 78(1) of the Hamburg Act). It was unanimously reported at the oral hearing that labelling was not currently being carried out in practice and that in any case, labelling on its own did not ensure that every single piece of data complied with the purpose limitation requirements. The situation appears to be particularly difficult in cases where databases are integrated automatically, especially where large datasets are involved. In such cases, purpose limitation requirements can only limit the amount of data by means of organisational and technical safeguards, which would have to be specified in greater detail in order to reduce the severity of interference to any significant degree under constitutional law. 139

Although the data protection provisions under § 20(4) of the Hesse Act, under § 66 of the Hessian Data Protection and Freedom of Information Act (*Hessisches Datenschutz- und Informationsfreiheitsgesetz*) and under § 56 of the Hamburg Act do require that organisational and technical safeguards be in place to ensure compliance with purpose limitation requirements, these provisions do not restrict the data that can be used in automated data analysis/interpretation with sufficient legal clarity and specificity. This would have to be addressed in greater detail – at least with regard to the powers under § 25a of the Hesse Act and § 49 of the Hamburg Act. Examples of technical and organisational safeguards designed to ensure compliance with purpose limitation requirements include the technical separation of datasets according to different processing purposes, and the granting of access rights to data depending on the purpose pursued ([...]). The *Land* Government of Hesse explained several times that different levels of access to the analysis platform are granted on the basis of a special role and rights-based concept ([...]). In principle, a concept of this type can be a suitable technical/organisational means of ensuring compliance with purpose limitation requirements, but no such concept has yet been cast into a regulatory framework and the legislator has yet to specify any requirements to this end. [...] 140

(bb) In principle, specialised rules concerning the further use of data obtained from particularly serious interferences with fundamental rights would also be capable of limiting the type and amount of usable data. For law enforcement data, § 479(2) second sentence of the Code of Criminal Procedure is particularly relevant in this respect. Similar provisions can be found in § 34(4) first sentence and § 36(2) second sentence of the Hamburg Act, while § 20(1) third sentence and (3) of the Hesse Act sets out requirements 141

for the further processing of personal data obtained from the surveillance of private homes and remote searches. But these provisions are not capable of significantly reducing the severity of interference of data analysis/interpretation since their applicability to automated data analysis/interpretation is not set out in a sufficient manner and their practical effect is not sufficiently guaranteed by rules on technical and organisational implementation.

(α) This is of particular relevance in cases where automated data analysis/interpretation makes use of traffic data from radio cell queries, which can give rise to very large datasets. At the oral hearing, the Federal Officer for Data Protection and Freedom of Information explained that for each radio cell query, a delivery containing around 100,000 pieces of data is produced. The Hessian Officer for Data Protection and Freedom of Information reported that data from the last two years of radio cell queries in Hesse was accessible. However, insofar as such data is collected under § 100g(3) of the Code of Criminal Procedure, its further use for the purpose of averting dangers is restricted by § 479(2) second sentence of the Code of Criminal Procedure. It is not immediately apparent whether an equivalent restriction would apply if radio cell data was collected not under the Code of Criminal Procedure but for preventive purposes under § 15a(5) fifth sentence of the Hesse Act. At the oral hearing, the Hessian Ministry of the Interior and Sports stated that traffic data was integrated into the data analysis platform only in cases under § 25a(1) second alternative of the Hesse Act – i.e. only when data analysis was conducted for the purpose of averting a danger to certain legal interests and not when it was conducted as a precautionary measure for the prevention of criminal offences. In this respect, the amount of traffic data that can be used in data analysis under § 25a(1) first alternative of the Hesse Act – the only constellation under review here – does appear to be limited, at least in practice. But here again, this limitation would have to be set out in sufficiently clear and transparent terms, especially since the safeguard mechanism of data labelling is evidently not being carried out at present (see para. 139 above). Insofar as the legislator itself is unable to specify the technical/organisational safeguards necessary to implement the exclusion of traffic data from data analysis, it must oblige the administrative authorities to specify and publish the appropriate technical details if it wishes to reduce the severity of interference resulting from automated data analysis in this manner. 142

(β) The same applies to the inclusion of other data obtained from particularly serious interferences. At the oral hearing, the Hessian Ministry of the Interior and Sports explained that such data (again due to § 479(2) second sentence of the Code of Criminal Procedure) was only included when data analysis was conducted under § 25a(1) second alternative of the Hesse Act – i.e. only when data analysis was conducted for the purpose of averting a danger to certain legal interests and not when it was conducted as a precautionary measure for the prevention of criminal offences. The amount of data that could be used in cases where data analysis was conducted as a precautionary measure for the prevention of criminal offences was therefore limited, at least in practice. 143

However, since the statements addressing this issue at the oral hearing all confirmed that data stored in the case management system is not currently being labelled, nor is this even possible, it remained unclear whether the police could find a workable method of screening information newly entered into the case management system (which is automatically integrated into the analysis platform) to ensure that data from serious interferences is reliably identified and filtered out prior to the automated data analysis process. In practice, one reason why no data is currently being filtered out of the case management system is that the entire dataset was supposed to be made available for automated data processing under § 25a of the Hesse Act because it contains data that is so new that it cannot be found in any other police systems ([...]); a filtering stage that would enable data from serious interferences to be separated out is not therefore conducted prior to the data analysis process ([...]). 144

Once again, there is a lack of provisions that clearly require data from particularly serious interferences to be filtered out before data analysis is conducted and that require technical/organisational safeguards to be implemented in order to ensure compliance with this filtering requirement. The severity of interference resulting from data analysis has not therefore been reduced in a sufficiently reliable manner. 145

(2) The severity of interference is specifically increased by the kind of data processing methods allowed by the challenged provisions. Based on their wording, § 25a of the Hesse Act and § 49 of the Hamburg Act permit the use of very far-reaching methods of automated data analysis/interpretation. The legislators have not restricted the permissible methods of analysis/interpretation. 146

(a) The challenged provisions do not rule out complex forms of data matching. When the wording in § 25a of the Hesse Act and § 49 of the Hamburg Act refers to automated data analysis/interpretation as opposed to, say, (automated) data cross-checking, a systematic distinction is already being made in the legislation (see § 25 of the Hesse Act and § 48(1) of the Hamburg Act). Unlike with rudimentary cross-checking, § 25a of the Hesse Act and § 49 of the Hamburg Act allow the police to engage in data mining processes (cf. BVerfGE 156, 11 <40 para. 74>) that can even encompass the use of self-learning systems (AI). What is more, the provisions also permit openly structured searches (see para. 93 ff. above). They allow the analysis/interpretation process to be solely directed at identifying distinctive statistical features in the available data, from which further conclusions can be drawn, possibly with the help of additional automated applications. Moreover, the provisions do not impose any limits on the search results that can be generated (see para. 96 ff. above). Based on the wording of the provisions, the search results could be made up of machine-driven evaluations, including assessments as to the level of danger posed by specific individuals in the manner of 'predictive policing'. Data analysis/interpretation can thus be used to generate new, otherwise inaccessible information that affects the personality rights of those concerned ([...]). The potential extent of this newly generated intelligence is not covered by rules regarding the use of such intelligence that would be capable of reducing the severity of interference. 147

(b) The legislator in Hamburg attempted to rule out such far-reaching applications by using the term ‘data interpretation’ instead of ‘data analysis’ ([...]). However, its intention of limiting the permitted range of applications is not significantly expressed in the wording of the legislation. The change in terminology from ‘data analysis’ to ‘data interpretation’ fails to indicate, in a constitutionally sufficient manner, that the analysis platform is limited to showing matches on the basis of specific search criteria and does not replace the data analysis and evaluation carried out by the police. No significant difference between the terms ‘data analysis’ and ‘data interpretation’ is discernible. Furthermore, § 49(2) of the Hamburg Act still refers to processing objectives that necessitate the use of data mining (cf. in this respect also BVerfGE 156, 11 <40 para. 74>). 148

(c) Nor are the challenged powers limited in any constitutionally relevant manner by the argument that the current state of technology does not allow the unlimited use of data interpretation. Whether this is actually the case need not be examined here, because even if a provision only enables the use of expanded capabilities once further technological developments have taken place, the constitutional requirements must still in principle be based on those expanded capabilities. The severity of interference resulting from a provision is not determined by the legislator’s ability to envisage the potential limits to the reach of the conferred powers, nor is it affected by the fact that the administrative authorities have no intention of making extensive use of the legal possibilities available thereunder. Rather, the severity must be determined according to the interferences that are legally possible. If the legislator had wanted to significantly limit the severity of interference, it should have made this explicitly clear in the wording of the provision (cf. Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 325 f.). 149

bb) The legislators in Hesse and Hamburg have thus imposed virtually no restrictions on the powers to conduct automated data analysis/interpretation under § 25a of the Hesse Act and § 49 of the Hamburg Act. These provisions authorise the police to interfere with fundamental rights in potentially very serious ways. The powers in question allow the automated processing of unlimited amounts of data, using methods that are not circumscribed by law. Given the lack of restrictions in terms of the usable data and the permissible methods, the provisions enable the police to create comprehensive profiles of persons, groups and circles with a single click. The provisions can also result in large numbers of legally uninvolved persons being subjected to further police measures if their data was collected in some particular context and the automated evaluation of this data leads the police to wrongly identify them as suspects. 150

For these reasons, the constitutional requirements that apply here are the same as for surveillance measures by public security authorities that result in deep intrusions into the private sphere. The generally applicable threshold for the use of covert surveillance measures by public security authorities is the existence of an identifiable danger (cf. Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 248 with further references; for specific details BVerfGE 141, 220 <272 f. para. 112>; 154, 152 <268 para. 219> and para. 106 above) to particularly weighty legal in- 151

terests (cf. BVerfGE 141, 220 <270 para. 108> and para. 105 above). As was described in considerable detail at the oral hearing, the fact that the legal possibilities available under the powers are not fully exploited in practice, are not meant to be fully exploited and indeed cannot be fully exploited due to the current state of technology does not alter the constitutional requirements.

III.

Based on these standards, § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act do not satisfy the requirements arising from the principle of proportionality in the strict sense because they do not contain sufficient thresholds for interference. Pursuant to § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act, the further processing of data by means of automated data analysis/interpretation is permissible in justified individual cases if this is necessary to prevent the criminal offences listed in § 100a(2) of the Code of Criminal Procedure. According to the definitions in § 1(1) second sentence no. 1 of the Hamburg Act and § 1(4) of the Hesse Act, the 'prevention of criminal offences' encompasses the deterrence of criminal offences (or 'expected' criminal offences in the case of the Hesse Act) (see 1. below) as well as precautionary measures for the prosecution of future criminal offences (see 2. below). In both alternatives, the grounds for interference are a long way short of the constitutionally required threshold of an identifiable danger. The question of whether the legislator has specified legal interests of sufficient weight does not need to be decided here (see para. 48 above). 152

1. Insofar as § 25a(1) first alternative in conjunction with § 1(4) of the Hesse Act and § 49(1) first alternative in conjunction with § 1(1) second sentence no. 1 of the Hamburg Act authorise data analysis/interpretation for the purpose of preventing the criminal offences listed in § 100a(2) of the Code of Criminal Procedure, the specified grounds for interference are disproportionately broad given the severity of interference, and the provisions are therefore unconstitutional. 153

a) In permitting the use of automated data analysis/interpretation for the purpose of preventing serious criminal offences generally, the provisions fail to lay down sufficiently restrictive grounds for interference and they lack the necessary threshold of an at least identifiable danger (cf. also BVerfGE 141, 220 <336 para. 313>; Federal Constitutional Court, Judgment of the First Senate of 26 April 2022 - 1 BvR 1619/17 -, para. 375). While § 1(4) of the Hesse Act does include the additional qualifier of 'expected' criminal offences, this still falls a long way short of the required threshold of an identifiable danger. Indeed, the description of the police's responsibilities in § 1(4) of the Hesse Act is deliberately intended to expand the scope of the police's remit in both temporal and substantive terms, extending it beyond the purpose of averting dangers as formulated in § 1(1) of the Hesse Act and moving away from the attachment to specific criminal offences ([...]). 154

b) Moreover, even though both provisions include the additional requirement that automated data processing only be carried out in justified 'individual cases', this require- 155

ment contains virtually no further substantive determinations.

aa) Firstly, the requirement that automated data processing only be carried out in individual cases is not formulated in sufficiently specific terms. It is not even clear what the criterion of an 'individual case' refers to. Responding in a different context to a question concerning § 25a(3) of the Hesse Act, the Hessian Minister of the Interior and Sports explained that an individual case within the meaning of § 25a of the Hesse Act refers not to an individual investigation but rather to a 'procedure or project linked to an investigation' (cf. Hessian state parliament documents, *Hessischer Landtag Drucksachen* – HessLT-Drucks 20/660, p. 1 f.). However, as an interpretation of 'individual case', neither the particularly broad definition of a 'project' nor the somewhat narrower definition of an 'individual investigation' satisfy the constitutional requirement applicable here, namely that every further use of every single piece of data must be of significance for averting an at least identifiable danger (cf. BVerfGE 150, 244 <286 f. para. 108>). That said, as the Hessian Ministry of the Interior and Sports explained at the oral hearing, checks are carried out before every data analysis measure to ensure compliance with the prerequisites of § 25a of the Hesse Act. This practice would nevertheless have to be set out in a clear legal framework. 156

bb) At any rate, the requirement that automated data processing only be carried out on in justified 'individual cases' falls short of the constitutionally required threshold of an at least identifiable danger. 157

(1) It is true that by subjecting every single data analysis/interpretation measure to a case-by-case assessment – the 'individual case' requirement –, the purely speculative use of automated data analysis/interpretation is ruled out (cf. BVerfGE 130, 151 <205>) and the police are prevented from using mass data processing to generate entirely new factual indications of future criminal offences without any grounds for suspicion. The requirement of a case-by-case assessment is thus roughly equivalent to the prerequisite that data provide a lead for further investigations (cf. BVerfGE 141, 220 <325 f. para. 281>). In practice, the simple fact that data and datasets have to be individually assessed before being included in data analysis/interpretation and the fact that their inclusion must be necessary for the specific preventive measure in question might have a certain limiting effect (cf. BVerfGE 130, 151 <205>). However, this still falls a long way short of the threshold of an at least identifiable danger. 158

(2) At the oral hearing, a somewhat narrower concept of how the 'individual case' criterion is understood and applied by the police in Hesse was outlined: data analysis is always linked to a criminal offence that has already been committed or, at a minimum, to the facts-based suspicion that a criminal offence has been committed. A prognosis for the future is then made on this basis. In order to carry out automated data analysis under this concept, the following two assumptions must be possible: first, that one of the criminal offences listed in § 100a(2) of the Code of Criminal Procedure has already been committed and, second, that on this basis, similar criminal offences are to be expected in future. 159

(a) By narrowing the 'individual case' criterion to constellations in which there are sufficient factual indications to support the assumption that a criminal offence has already been committed, the scope of application of § 25a(1) first alternative of the Hesse Act is restricted. It is true that the data analysis powers in § 25a(1) of the Hesse Act are formulated as being authorised for preventive purposes and, as such, may not be used by the police for law enforcement purposes due to the lack of a statutory basis. This is without even taking the question of legislative competence into consideration. Nevertheless, data analysis could potentially still be regarded as serving preventive purposes if the assessment of the suspicion that a criminal offence has been committed merely serves to ascertain whether similar criminal offences are likely to be committed in future. In practical terms, this means that data analysis can be considered an option primarily when dealing with criminal offences that are usually committed in series, so that if one criminal offence is committed, it is possible under certain circumstances to infer that further criminal offences will follow. This further narrows the scope of application of § 25a(1) first alternative of the Hesse Act. 160

(b) However, if the conclusion that a certain criminal offence might be committed in future is merely based on the abstract assumption that certain criminal offences are often committed in series, the scope of application would not be restricted to the same extent. To satisfy the requirement of a case-by-case assessment, the specific circumstances of the individual criminal offence that has been committed (or is suspected of having been committed) must be closely examined in order to ascertain whether the commission of similar offences can be expected in future. According to statements made at the oral hearing, the practice in Hesse is to closely examine the specific circumstances that prompted the suspicion that a criminal offence has been committed and then, based on empirical knowledge of criminal behaviour, to predict the probability of further criminal offences being committed; this kind of approach to implementing the provision would serve to restrict its scope of application. But it also emerged at the oral hearing that the police in Hesse, working on the basis of generalisations, have identified certain fields of criminal activity in which further crimes are generally expected to occur and for which the assumption in every single case is that further criminal offences are imminent; this approach undermines the restrictive effect. Since the practice in Hesse is not documented in a publicly accessible form, this cannot be reviewed in greater detail here. 161

(c) The restrictive effect is furthermore weakened if, in the individual case, there is no detailed examination of whether the individual pieces of data used in the analysis are suitable to help prevent a potentially imminent serial offence. In principle, data processing measures only satisfy the proportionality requirements if the personal data to be used is required to have potential significance for the purpose of the specific measure (cf. BVerfGE 150, 244 <286 f. para. 108 f.>). This is because if data analysis/interpretation is authorised for the purpose of preventing certain criminal offences, this purpose also defines the limits applicable to each individual data analysis and data matching step. If datasets unrelated to this purpose are to be used in data analysis/interpretation, a separate and sound reason would be required. Absent any such reason, it is disproportion- 162

ate to use datasets that, from the outset, cannot serve the purpose of the specific data analysis/interpretation measure (cf. BVerfGE 150, 244 <288 para. 111>).

163 In Hesse, case-by-case assessments to evaluate the suitability of the available data do appear to be an established concept in practice. During the oral hearing, however, the Hessian Ministry of the Interior and Sports explained that all the data available in the analysis platform, including the data from the case management system, is routinely considered suitable on the assumption that it is generally suitable for helping to achieve the intelligence objectives of the individual case. The data's specific suitability does not appear to be examined in any greater detail. Indeed, given the vast amounts of data in Hesse resulting from the inclusion of case management data, it is hard to imagine how a suitability assessment could, in practice, be conducted for each piece of data. This makes it all the more important to have a clear legal framework, backed up by transparent technical and organisational safeguards, specifying what data can in fact be included in each individual data analysis measure.

164 (d) Despite the detailed structuring of this police practice in Hesse, the constitutional requirements are not met because, from the outset, the concept is not oriented towards the threshold of an at least identifiable danger and towards the data suitable for averting such a danger. Yet this is necessary given the broadly worded nature of § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act as regards the usable data and the permissible methods.

165 If, on the other hand, the powers were to be more narrowly defined in terms of the type and scope of the usable data and the permissible methods of data processing, thereby reducing the potential severity of interference to such an extent that a lower threshold for exercising the powers would suffice under constitutional law (see para. 75 ff. and 107 above), the concept that currently informs the police practice in Hesse could serve as a starting point for designing the thresholds for interference in conformity with the Constitution. The specific aspects of this cannot and need not be decided here. However, such a concept would have to be cast into a detailed legal framework in compliance with the principle that interferences be based on statutory provisions and the principles of legal clarity and specificity. At present, § 25a of the Hesse Act does not in any way set out the concept used by the police in Hesse.

166 cc) The *Land* Governments of Hesse and Hamburg are correct in submitting that in other cases involving security law, the Federal Constitutional Court has found a case-by-case assessment to be a sufficient requirement. Indeed, case-by-case assessments are unproblematic when serving to further elaborate a threshold that has already been established using other criteria (cf. BVerfGE 141, 220 <272 para. 112>). Particularly in cases where a provision requires that a measure be necessary in the individual case to avert a danger, a case-by-case assessment can replace a more precise description of the required level of danger and can constitute a sufficiently detailed definition of the requirement that a specific danger be present – provided that the provision does not authorise any particularly serious interferences with fundamental rights (cf. BVerfGE 130, 151

<205>; 155, 119 <192 para. 158>). When it comes to interferences by the intelligence services, which must always serve to protect particularly weighty legal interests, the requirement of a case-by-case assessment can provide a constitutionally sufficient mechanism for verifying whether the actual threshold for conducting surveillance of an activity or endeavour that warrants observation has been reached – provided that the measure itself does not intrude deeply intrude into the private sphere (cf. BVerfGE 130, 151 <206>; 155, 119 <189 para. 151>; 156, 11 <59 para. 126>; Federal Constitutional Court, Judgment of the First Senate Judgment of 26 April 2022 - 1 BvR 1619/17 -, para. 206). However, none of this is applicable here.

The challenged provisions differ in this respect from § 6a(3) of the Counter-Terrorism Database Act, which is compatible with the Basic Law. That provision, which authorises the extended use of data, likewise makes reference to the concept of the individual case. However, it imposes stricter requirements. It provides that an involved federal authority, in the discharge of its statutorily assigned tasks, is permitted to make extended use of the types of data stored in the counter-terrorism database insofar as this is necessary – in the context of conducting a specific case-related project aimed at preventing certain qualified types of international terrorist offences – to clarify further circumstances of the individual case, provided that facts justify the assumption that such an offence is going to be committed. In several respects, this is narrower than § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act. Particularly significant is the fact that extended use of the counter-terrorism database must be necessary to 'clarify further circumstances of the individual case'. Based on an interpretation of § 6a(3) of the Counter-Terrorism Database Act in conformity with the Constitution, this is understood as meaning that further use of the database is only permitted if the authority can at least determine the type of identifiable and foreseeable incident that might occur, or if the authority recognises that the individual conduct of a person establishes the specific probability that they will commit terrorist offences in the not so distant future. Extended use therefore requires a danger that is identifiable as set out above, the further investigation of which must require such use in a sufficiently clear manner (BVerfGE 156, 11 <61 para. 130>). These restrictive prerequisites are lacking in § 25a of the Hesse Act and § 49 of the Hamburg Act. 167

c) Regarding the legal situation in Hamburg, it cannot be argued that the powers under § 49(1) first alternative of the Hamburg Act are subject to the necessary restrictions by virtue of other provisions elsewhere in the Act. It is true that § 11(1) no. 6 of the Hamburg Act does tie the processing of personal data – which includes data interpretation under § 49 of the Hamburg Act (cf. § 2(8) of the Hamburg Act) – to certain conditions when carried out for the purpose of preventing criminal offences: first, that factual indications justify the assumption that the person in question will commit criminal offences in future, and second, that data processing is necessary as a precautionary measure to prevent considerable criminal offences. From a systematic perspective, this could potentially be understood as establishing a permanently applicable minimum requirement for the processing of personal data conducted for the purpose of preventing criminal of- 168

fences. However, the Hamburg legislator regards § 49 of the Hamburg Act as a special provision that is intended to be exempt from the generally applicable requirement set out in § 11(1) no. 6 of the Hamburg Act. This view, which was reiterated at the oral hearing, is a fundamental legislative decision and is to be respected as such. Any understanding that deviates from this view would be incompatible with that decision.

d) Furthermore, the requirement that data analysis/interpretation be limited to cases involving an at least identifiable danger, which is mandated by constitutional law here in view of the specific design of the challenged powers, is not satisfied by only permitting data analysis/interpretation to be carried out in 'justified' individual cases. Even if the powers were to be more narrowly defined in some future legislation and a lower threshold for interference would thus be sufficient, it is not clear whether the criterion of a 'justified' individual case would be capable of curtailing the reach of the powers in question. Nor is it discernible that this criterion gives rise to any further substantive requirements. At the oral hearing, the Hessian Ministry of the Interior and Sports stated that in order for an individual case to be justified, it must be backed up by sufficiently tangible facts of a twofold nature (see para. 159 above). Yet this goes no further than the requirements already derived from the principle of a case-by-case assessment in Hessian police practice and, moreover, lacks a statutory basis given that the terms 'justified' and 'individual case' provide no legislative support for this interpretation. As the oral hearing also made clear, this aspect does not require that a written explanation be provided for the measure in question (see para. 109 above on the necessity thereof), nor does it give rise to any other procedural requirements. Overall, it is not therefore discernible that the criterion of a 'justified' individual case serves to limit the powers with sufficient clarity. 169

e) Moreover, § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act both fail to set out a sufficient threshold in that the catalogue of offences in § 100a(2) of the Code of Criminal Procedure also incorporates preparatory acts in the form of potential threats to certain legal interests. Given the severity of interference, shifting the threshold for exercising the powers in question to a purely precautionary stage before any legal interests have been specifically endangered or violated is incompatible with the Constitution if it means that such powers could be exercised at this stage on grounds of relatively vague indications of possible impairments of legal interests (cf. BVerfGE 141, 220 <273 para. 113> with further references). Tying the threshold for interference to the danger of criminal offences being committed is not therefore necessarily in line with constitutional requirements if, due to the incorporation of preparatory acts, the criminal offences in question are already punishable before any specific dangers to a relevant legal interest have arisen and before any violations have occurred. It is true that the commission of a preparatory act can itself constitute an identifiable or specific danger to the protected legal interest in question. This is not certain, however; on its own, the mere risk that a preparatory act will be committed does not necessarily pose any such danger to a legal interest. Yet a danger to a protected legal interest is precisely what is required. It is true that the legislator is not prevented under constitutional law from tying the prerequisites for interference to the danger that a preparatory act will 170

be committed. However, the legislator must then ensure that in each individual case, the requisite specific or identifiable danger to the legal interest protected by the referenced offence does actually exist. Thus, if the legislator ties the threshold for exercising the powers in question to the commission of such an offence, it must also insist that an identifiable or specific danger to the legal interest protected by the referenced offence has already arisen (cf. Federal Constitutional Court, Order of the First Senate of 28 September 2022 - 1 BvR 2354/13 -, para. 134; Order of the First Senate of 9 December 2022 - 1 BvR 1345/21 -, para. 92). This is lacking here.

2. According to the statutory definitions in § 1(4) of the Hesse Act and § 1(1) second sentence no. 1 of the Hamburg Act, the prevention of criminal offences within the meaning of § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act encompasses not just the deterrence of criminal offences, but also precautionary measures for the prosecution of future criminal offences. The aim is to enable the police to use automated data analysis to process their stored data in order to gain insights for future intelligence work and investigations ([...]). It is not evident that a specific danger or an identifiable danger is required. Here again, there is a lack of any specific restrictions on the grounds for interference (cf. also BVerfGE 141, 220 <336 para. 313>). 171

The Hamburg Government's argument that § 49(1) of the Hamburg Act has nothing to do with precautionary measures for the prosecution of future criminal offences because its applicability is limited to 'justified individual cases' cannot be accepted in view of the clear definition in § 1(1) second sentence no. 1 of the Hamburg Act. Rather, precautionary measures that serve law enforcement purposes would have to be explicitly ruled out. 172

D.

I.

Ultimately, § 25a(1) first alternative of the Hesse Act and § 49(1) first alternative of the Hamburg Act are unconstitutional. They violate the general right of personality (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law) in its manifestation as the right to informational self-determination because they do not contain thresholds that are appropriate to the severity of interference resulting from the authorised data analysis/interpretation measures. [...] 173

II.

1. The finding that a statutory provision is unconstitutional generally results in that provision being declared void. However, pursuant to § 31(2) second and third sentence of the Federal Constitutional Court Act, the Federal Constitutional Court may limit its decision to declaring that an unconstitutional provision is merely incompatible with the Constitution. It then merely objects to the unconstitutional provision without declaring it void. The Court may combine the declaration of incompatibility with a temporary order 174

to continue to apply the unconstitutional provisions. This may be considered in cases where the immediate invalidity of the objectionable provision would eliminate the statutory basis for protecting exceptionally significant interests of the common good, and if a balancing of these interests against the affected fundamental rights requires that the interference be tolerated for a transitional period. During the transitional period, the Federal Constitutional Court may issue interim orders to reduce the powers of the authorities, in line with what appears necessary in light of its balancing, until a situation of constitutional conformity has been established (BVerfGE 141, 220 <351 para. 355> with further references; established case-law).

2. In accordance with the above, § 25a(1) first alternative of the Hesse Act is merely declared incompatible with the Constitution. The declaration that the provision is incompatible with the Constitution is combined with the order that it is nonetheless to stay in effect on an interim basis until the legislator has enacted new provisions, or until 30 September 2023 at the latest. The provision may no longer be applied after that date. Given the significance that the legislator may accord to the powers in question for the exercise of state functions, given the significance of the powers for the Hessian police's precautionary work to prevent criminal offences, and given the fact that the Hessian police – despite making regular use of these powers – have not thus far made any use of their more far-reaching possibilities, thereby minimising the impact on fundamental rights, a temporary application of the provision is preferable to a declaration of voidness. 175

However, in ordering the continued applicability of the provision, it is necessary to impose certain restrictions to protect the affected fundamental rights. These, however, do not predetermine the new provisions to be enacted by the legislator. Based on the concept used by the police in Hesse, the powers under § 25a(1) first alternative of the Hesse Act may only be used on condition that sufficiently specific facts give rise to the suspicion (cf. BVerfGE 154, 152 <268 para. 219>; 156, 11 <56 para. 120>) that a particularly serious criminal offence within the meaning of § 100b(2) of the Code of Criminal Procedure has been committed and it is expected, given the particular circumstances of the suspicion in the individual case, that similar criminal offences will be committed that will jeopardise the life and limb of persons or the existence or security of the Federation or a *Land*. Furthermore, the existence of these requirements and the specific suitability of the data used under § 25a(1) first alternative of the Hesse Act to prevent the expected criminal offence must be confirmed in a written explanation in each individual case; it must also be ensured that no information is used that was obtained from the surveillance of private homes, remote searches, telecommunications surveillance, traffic data retrieval, longer-term observations, the use of undercover investigators or confidential informants, or from similarly serious interferences with the right to informational self-determination. 176

3. § 49(1) first alternative of the Hamburg Act, on the other hand, is declared unconstitutional and void because there is nothing to suggest that a temporary order of continued application would be necessary or justified. There is no evidence that the police intend to use the powers under § 49(1) first alternative of the Hamburg Act in the short or 177

medium term to conduct precautionary measures for the effective prevention of criminal offences.

III.

[...] 178

Harbarth Baer Britz

Ott Christ Radtke

Härtel Wolff

Bundesverfassungsgericht, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20

Zitiervorschlag BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20 - Rn. (1 - 178), http://www.bverfg.de/e/rs20230216_1bvr154719en.html

ECLI ECLI:DE:BVerfG:2023:rs20230216.1bvr154719