Leitsätze

zum Urteil des Ersten Senats vom 16. Februar 2023

- 1 BvR 1547/19 -

- 1 BvR 2634/20 -

Automatisierte Datenanalyse

1. **Werden gespeicherte Datenbestände mittels einer automatisierten Anwendung zur Datenanalyse oder -auswertung verarbeitet, greift dies in die informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) aller ein, deren Daten bei diesem Vorgang personenbezogen Verwendung finden.**

2. **Das Eingriffsgewicht einer automatisierten Datenanalyse oder -auswertung und die Anforderungen an deren verfassungsrechtliche Rechtfertigung ergeben sich zum einen aus dem Gewicht der vorausgegangenen Datenerhebungseingriffe; insoweit gelten die Grundsätze der Zweckbindung und Zweckänderung. Zum andern hat die automatisierte Datenanalyse oder -auswertung ein Eigengewicht, weil die weitere Verarbeitung durch eine automatisierte Datenanalyse oder -auswertung spezifische Belastungseffekte haben kann, die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen; insoweit ergeben sich aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne weitergehende Rechtfertigungsanforderungen.**

3. **Diese weitergehenden Anforderungen an die Rechtfertigung einer automatisierten Datenanalyse oder -auswertung variieren, da deren eigene Eingriffsintensität je nach gesetzlicher Ausgestaltung ganz unterschiedlich sein kann. Das Eingriffsgewicht wird insbesondere durch Art und Umfang der verarbeitbaren Daten und die zugelassene Methode der Datenanalyse oder -auswertung bestimmt. Der Gesetzgeber kann die Eingriffsintensität durch Regelungen zu Art und Umfang der Daten und zur Begrenzung der Auswertungsmethode steuern.**

4. **Ermöglicht die automatisierte Datenanalyse oder -auswertung einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung, ist dies nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten, also nur zum Schutz besonders gewichtiger Rechtsgüter, sofern für diese eine zumindest hinreichend konkretisierte Gefahr besteht. Das Erfordernis einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter ist nur dann verfassungsrechtlich verzichtbar, wenn die zugelassenen Analyse- und Auswertungsmöglichkeiten durch Regelungen insbesondere zur Begrenzung von Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden normenklar und hinreichend bestimmt in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahmen erheblich gemindert ist.**

5. **Grundsätzlich kann der Gesetzgeber den Erlass der erforderlichen Regelungen zu Art und Umfang verarbeitbarer Daten und zu den zulässigen Datenverarbeitungsmethoden zwischen sich und der Verwaltung aufteilen. Er muss aber sicherstellen, dass unter Wahrung des Gesetzesvorbehalts insgesamt ausreichende Regelungen getroffen werden.**

a. **Der Gesetzgeber muss die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben.**

b. **Soweit er die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigt, hat der Gesetzgeber zu gewährleisten, dass die Verwaltung die für die Durchführung einer automatisierten Datenanalyse oder -auswertung im Einzelfall maßgeblichen Vorgaben und Kriterien in abstrakt-genereller Form festlegt, verlässlich dokumentiert und in einer vom Gesetzgeber näher zu bestimmenden Weise veröffentlicht. Das sichert auch die verfassungsrechtlich gebotene Kontrolle, die insbesondere durch Datenschutzbeauftragte erfolgen kann.**

BUNDESVERFASSUNGSGERICHT

- 1 BvR 1547/19 -

- 1 BvR 2634/20 -

Verkündet
am 16. Februar 2023
Hoffmann
Regierungshauptsekretär
als Urkundsbeamter
der Geschäftsstelle

IM NAMEN DES VOLKES

**In den Verfahren
über
die Verfassungsbeschwerden**

I. 1. der Frau (…),

2. des Herrn (…),

3. der Frau (…),

4. des Herrn (…),

5. des Herrn (…),

- Bevollmächtigte: 1. Prof. Dr. Tobias Singelnstein,
(…)
- Bevollmächtigter zu Ziffer 1 bis 5 -

2. Rechtsanwältin Sarah Lincoln,
(…)
- Bevollmächtigte zu Ziffer 3 -

gegen § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018

(Gesetz- und Verordnungsblatt Hessen Seite 302)

- 1 BvR 1547/19 -,

II. 1. der Frau (…),

2. der Frau (…),

3. der Frau (…),

4. der Frau (…),

5. der Frau (…),

6. des Herrn (…),

- Bevollmächtigte: 1. Jun.-Prof. Dr. Sebastian Golla,
Universitätsstraße 150, 44801 Bochum
- Bevollmächtigter zu Ziffer 1 bis 6 -

2. Rechtsanwalt Dr. Bijan Moini,
(…)
- Bevollmächtigter zu Ziffer 6 -

gegen § 49 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei (PolDVG) in der Fassung des Gesetzes über die Datenverarbeitung der Polizei und zur Änderung weiterer polizeirechtlicher Vorschriften vom 12. Dezember 2019 (Gesetz- und Verordnungsblatt Hamburg Seite 485)

- 1 BvR 2634/20 -

hat das Bundesverfassungsgericht – Erster Senat –

unter Mitwirkung der Richterinnen und Richter

Präsident Harbarth,

Baer,

Britz,

Ott,

Christ,

Radtke,

Härtel,

Wolff

aufgrund der mündlichen Verhandlung vom 20. Dezember 2022 durch

Urteil

für Recht erkannt:

1. **§ 49 Absatz 1 Alternative 1 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei (PolDVG) in der Fassung des Gesetzes über die Datenverarbeitung der Polizei und zur Änderung weiterer polizeirechtlicher Vorschriften vom 12. Dezember 2019 (Gesetz- und Verordnungsblatt Hamburg Seite 485) verstößt gegen Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes und ist nichtig.**

   Im Übrigen wird die Verfassungsbeschwerde im Verfahren 1 BvR 2634/20 zurückgewiesen.

   Die Freie und Hansestadt Hamburg hat den Beschwerdeführenden zwei Drittel ihrer notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren 1 BvR 2634/20 zu erstatten.

2. **§ 25a Absatz 1 Alternative 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018 (Gesetz- und Verordnungsblatt Hessen Seite 302) ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar.**

   Bis zu einer Neuregelung, längstens jedoch bis zum 30. September 2023, gilt § 25a Absatz 1 Alternative 1 des Gesetzes über die öffentliche Sicherheit und Ordnung mit den folgenden Maßgaben fort: Eine Datenanalyse nach § 25a Absatz 1 Alternative 1 des Gesetzes über die öffentliche Sicherheit und Ordnung darf nur durchgeführt werden, wenn bestimmte, genügend konkretisierte Tatsachen den Verdacht begründen, dass eine besonders schwere Straftat im Sinne von § 100b Absatz 2 der Strafprozessordnung begangen wurde und aufgrund der konkreten Umstände eines solchen im Einzelfall bestehenden Verdachts für die Zukunft mit weiteren, gleichgelagerten Straftaten zu rechnen ist, die Leib, Leben oder den Bestand oder die Sicherheit des Bundes oder eines Landes gefährden, wenn das Vorliegen dieser Voraussetzungen und die konkrete Eignung der verwendeten Daten zur Verhütung der zu erwartenden Straftat durch eigenständig auszuformulierende Erläuterung begründet wird und wenn sichergestellt ist, dass keine Informationen in die Datenanalyse einbezogen werden, die aus Wohnraumüberwachung, Online-Durchsuchung, Telekommunikationsüberwachung, Verkehrsdatenabfrage, länger andauernder Observation, unter Einsatz von verdeckt ermittelnden Personen oder Vertrauenspersonen oder aus vergleichbar schwerwiegenden Eingriffen in die informationelle Selbstbestimmung gewonnen wurden.

Im Übrigen wird die Verfassungsbeschwerde im Verfahren 1 BvR 1547/19 zurückgewiesen.

Das Land Hessen hat den Beschwerdeführenden zwei Drittel ihrer notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren 1 BvR 1547/19 zu erstatten.

Inhaltsverzeichnis

G r ü n d e :

A.

Die Verfassungsbeschwerden betreffen landesrechtliche Ermächtigungen der Polizei zur automatisierten Datenanalyse oder -auswertung. 1

I.

Die beiden weitgehend gleichlautenden Regelungen in § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018 (GVBl Hessen S. 302) und in § 49 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei (im Folgenden: HmbPolDVG) in der Fassung des Gesetzes über die Datenverarbeitung der Polizei und zur Änderung weiterer polizeirechtlicher Vorschriften vom 12. Dezember 2019 (GVBl Hamburg S. 485) schaffen vor dem Hintergrund erweiterter technischer Möglichkeiten, Informationstechnologie auch in der polizeilichen Arbeit zu nutzen, eine spezielle Rechtsgrundlage dafür, bisher unverbundene, automatisierte Dateien und Datenquellen in Analyseplattformen zu vernetzen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen, um die polizeiliche Aufgabenerfüllung auf diese Weise zu erleichtern und zu verbessern (HessLTDrucks 19/6502, S. 41; s. auch Hamburgische Bürgerschaft AusschussDrucks 21/39, S. 10). 2

Die Vorschriften ermächtigen die Polizei, in begründeten Einzelfällen zur vorbeugenden Bekämpfung schwerer Straftaten im Sinne von § 100a Abs. 2 StPO (Alternative 1) oder zur Abwehr von Gefahren für bestimmte Rechtsgüter (Alternative 2) gespeicherte personenbezogene Daten mittels automatisierter Anwendung im Rahmen einer Datenanalyse (Hessen) oder einer Datenauswertung (Hamburg) weiter zu verarbeiten. Auf diese Weise können nach Absatz 2 der jeweiligen Regelung insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden. Verwandte Ermächtigungen für die Sicherheitsbehörden, die thematisch enger gefasst sind, bestehen auf Bundesebene, werden aber bislang nicht genutzt (§ 7 des Gesetzes zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus und § 6a des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern, Antiterrordateigesetz – ATDG; dazu BVerfGE 156, 11 – Antiterrordateigesetz II). 3

II.

1. Die am 4. Juli 2018 in Kraft getretene, im Verfahren 1 BvR 1547/19 angegriffene Regelung des § 25a HSOG hat folgenden Wortlaut: 4

§ 25a HSOG

Automatisierte Anwendung zur Datenanalyse

(1) Die Polizeibehörden können in begründeten Einzelfällen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten zur vorbeugenden Bekämpfung von in § 100a Abs. 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind.

(2) Im Rahmen der Weiterverarbeitung nach Abs. 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(3) [1]Die Einrichtung und wesentliche Änderung einer automatisier-

ten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten. [2]Die oder der Hessische Datenschutzbeauftragte ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen.

2. Der seit dem 24. Dezember 2019 gültige, im Verfahren 1 BvR 2634/20 angegriffene § 49 HmbPolDVG lautet wie folgt: 5

§ 49 HmbPolDVG

Automatisierte Anwendung zur Auswertung vorhandener Daten

(1) Die Polizei darf in begründeten Einzelfällen in polizeilichen Dateisystemen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenauswertung verarbeiten, wenn dies zur vorbeugenden Bekämpfung von in § 100a Absatz 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist.

(2) Im Rahmen der Verarbeitung nach Absatz 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(3) [1]Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung nach Absatz 1 erfolgen durch Anordnung der Polizeipräsidentin oder des Polizeipräsidenten oder der Vertretung im Amt. [2]Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen.

III.

Mit § 25a HSOG wurde erstmals eine landesrechtliche Befugnis zur automatisierten Datenanalyse geschaffen. Der hessische Gesetzgeber griff damit eine in Hessen bereits etablierte polizeiliche Praxis auf. Von den Befugnissen des § 25a HSOG wird jährlich tausendfach Gebrauch gemacht. § 49 HmbPolDVG wurde § 25a HSOG mit kleinen Abweichungen nachgebildet, wird aber bislang nicht angewendet. 6

1. Bereits 2017 hatte Hessen das Programm „Gotham“ vom Software-Unternehmen Palantir erworben und unter dem Namen „hessenDATA“ eingesetzt. Der Landesgesetzgeber entschied sich 2018, hierfür eine eigene Rechtsgrundlage zu schaffen, um insbesondere dem Recht auf informationelle Selbstbestimmung Rechnung zu tragen (HessLTDrucks 19/6502, S. 41). 7

In der Begründung des Gesetzentwurfs zu § 25a HSOG wird darauf verwiesen, dass ohne den Rückgriff auf derartige automatisierte Anwendungen wegen eines unverbundenen Nebeneinanders zahlreicher automatisierter Verfahren, Daten und Informationssysteme mit unterschiedlichen Zweckbindungen, Nutzerkreisen, Datenarten und Betroffenenkreisen wesentliche Anhaltspunkte für Gefahren und bevorstehende Straftaten in der aktuellen „IT-Struktur“ der Polizei verborgen blieben; insbesondere im Verlauf der bundesweiten Mordserie der „NSU“-Gruppe hätten sich Probleme im Informationsfluss gezeigt. Die Einrichtung und Nutzung eines automatisierten „Analysetools“ könne die polizeiliche Aufgabenerfüllung erheblich erleichtern und verbessern. Eine umfassende Analyse der verfügbaren Daten sei gerade für die Bekämpfung schwerer Straftaten geboten. Die Polizei könne so über die bisherigen Erkenntnismöglichkeiten hinaus Zusammenhänge sowie Handlungsmuster und damit auch künftiges strafbares oder gefährliches Verhalten von Personen erkennen und geeignete präventive Maßnahmen treffen (HessLTDrucks 19/6502, S. 40 f.). 8

§ 25a HSOG regele die automatisierte Analyse bereits rechtmäßig erlangter personenbezogener Daten. Die allgemeinen Regelungen des § 20 HSOG zur Datenweiterverarbeitung, zur Zweckbindung, zum Grundsatz der hypothetischen Datenneuerhebung und besondere Verwendungsregelungen seien zu beachten. Welche Datenbestände für die Datenanalyse erforderlich seien, müsse im Hinblick auf den jeweiligen Analysezweck geprüft und gegebenenfalls über Zugriffsberechtigungen definiert werden (HessLTDrucks 19/6502, S. 41). 9

Auf Grundlage der am 4. Juli 2018 in Kraft getretenen Regelung hat es nach Auskunft des Hessischen Innenministers bis Juni 2019 fünf „generelle phänomenbezogene Anordnungen“ gemäß § 25a Abs. 3 HSOG gegeben. Im Schwerpunkt erfolge ein Einsatz des Datenanalyseinstruments zur Abwehr terroristischer Gefahren bei Staatsschutzdienststellen sowie zur Bekämpfung der organisierten Kriminalität und der schweren Kriminalität (HessLTDrucks 20/660, S. 1 f.). Weitere Anordnungen nach § 25a Abs. 3 HSOG hat es nach Auskunft des Hessischen Beauftragten für Datenschutz und Informationsfreiheit seit 2019 nicht mehr gegeben; hessenDATA werde derzeit auf Grundlage der ersten fünf Anordnungen genutzt. 10

Der Hessische Innenminister hat außerdem berichtet, die Analyseplattform greife automatisiert auf die drei Datenbanken POLAS (polizeiliches Auskunftssystem für „repressive“ Daten), ComVor (Vorgangsbearbeitungssystem für sämtliche Verfahren) und CRIME-ST (Fallbearbeitungssystem zur Speicherung „präventiver“ Daten für künftige Ermittlungsverfahren) zu (HessLTDrucks 20/660, S. 2). Die relevanten Daten würden dabei automatisiert auf die Analyseplattform übertragen; sie würden in 11

regelmäßigem Abstand synchronisiert, was auch die Einhaltung der Löschfristen sicherstelle (HessLTDrucks 20/661, S. 2). Als weitere Datenquellen würden die Verkehrsdaten aus Telekommunikationsüberwachung und aus Abfragen (auch Funkzellenabfragen) bei den Telekommunikationsanbietern genutzt. Außerdem würden sogenannte „forensische Extrakte“, also etwa polizeilich beschlagnahmte Mobiltelefone, ausgewertet. Hinzu kämen Daten aus polizeilichen Fernschreiben, einer Art E-Mailsystem, in dem die Polizei hessenweit Informationen austausche (HessLTDrucks 19/6864, S. 18 f.). Quellsysteme anderer Länder, des Bundes oder anderer Staaten sowie öffentliche und andere nicht öffentliche Quellen seien nicht automatisiert eingebunden, könnten aber im Rahmen der gesetzlichen Möglichkeiten angefordert und dann integriert und ausgewertet werden. Gleiches gelte im Einzelfall auch für Daten aus präventivpolizeilichen und strafprozessualen Ermittlungsmaßnahmen wie etwa der Telekommunikations- oder der Wohnraumüberwachung sowie – unter der Voraussetzung eines vorherigen richterlichen Beschlusses – für die Daten aus sozialen Netzwerken. Ein direkter Zugriff auf soziale Netzwerke bestehe nicht, da aus Sicherheitsgründen vom Polizeinetz nicht direkt auf das Internet zugegriffen werde. Daten des Bundesamts für Verfassungsschutz oder der Landesämter für Verfassungsschutz würden nicht genutzt (zu allem HessLTDrucks 20/660, S. 2 f.; HessLTDrucks 19/6864, S. 18 f.).

Die Analyseplattform hessenDATA sei in das Netz der Polizei eingebunden und bei Bedarf von jedem Arbeitsplatz aus in Hessen technisch erreichbar. Ein Zugriff auf die gespeicherten Datensätze und deren Nutzung sei allerdings ausschließlich durch dafür gesondert geschultes Personal der Polizei möglich. Es handele sich im Schwerpunkt um Ermittelnde der Kriminalpolizei. Der Zugriff auf die Daten sei durch ein Rollen- und Rechtekonzept geregelt. Die Nutzer der Analyseplattform seien verschiedenen Gruppen zugeordnet, welche jeweils unterschiedliche Zugriffsrechte auf den analysierbaren, integrierten Datenbestand hätten. Die Einteilung der Nutzergruppen in der Analyseplattform erfolge automatisiert über die Zugehörigkeit der Mitarbeitenden zu ihrer Organisationseinheit (HessLTDrucks 20/661, S. 2). In der mündlichen Verhandlung wurde durch das Hessische Ministerium des Innern und für Sport dargelegt, dass derzeit insgesamt 2.099 Personen Zugriff auf hessenDATA hätten. Die Plattform werde pro Jahr in ungefähr 14.000 Fällen genutzt, davon in 2.000 Fällen nach § 25a Abs. 1 Alt. 2 HSOG, also zur Abwehr von Gefahren, und in 12.000 Fällen nach § 25a Abs. 1 Alt. 1 HSOG, also zur vorbeugenden Bekämpfung bestimmter Straftaten. 12

2. In Hamburg trat § 49 HmbPolDVG als Teil des durch das Gesetz über die Datenverarbeitung der Polizei und zur Änderung weiterer polizeirechtlicher Vorschriften (GVBl Hamburg S. 485) neu geschaffenen Hamburgischen Gesetzes über die Datenverarbeitung der Polizei am 24. Dezember 2019 in Kraft. Seine Entwurfsfassung orientierte sich stark an § 25a HSOG. Abweichend bestimmt war von Anfang an, dass es sich bei den gespeicherten personenbezogenen Daten nach Absatz 1 um in „polizeilichen Dateisystemen“ gespeicherte Daten handeln muss, während § 25a 13

HSOG schlicht von gespeicherten Daten spricht. Der Entwurf wurde im Rahmen des Gesetzgebungsverfahrens nach einer umfangreichen Anhörung sachverständiger Auskunftspersonen (Hamburgische Bürgerschaft AusschussDrucks 21/38) geändert. Der Hamburger Innensenator erklärte, man plane kein mit der Rasterfahndung vergleichbares Instrument, sondern eher eine Art qualifizierten Datenabgleich (Hamburgische Bürgerschaft AusschussDrucks 21/39, S. 9 f., 32). Zudem seien nach ausführlicher Prüfung ein „predictive policing“ oder die Anschaffung der hierfür erforderlichen Softwareprodukte nicht geplant. Es gehe vielmehr um eine erweiterte einzelfallbezogene Recherchemöglichkeit und die Möglichkeit, umfassender in den vorhandenen Systemen nach Treffern, Übereinstimmungen und Beziehungen zwischen unterschiedlichen Sachverhalten, die sonst vielleicht nicht sofort auffallen, suchen zu können, „einfach das, was sozusagen früher der Kriminalbeamte oder der Sachbearbeiter“ gemacht habe. Man versuche, so viele Informationen wie möglich zu einem Sachverhalt zusammenzutragen und dann Strukturen, Beziehungen und Übereinstimmungen herzustellen und daraus Schlüsse zu ziehen (Hamburgische Bürgerschaft AusschussDrucks 21/39, S. 25).

Im Gesetz wurde das in der Entwurfsfassung noch wie in der hessischen Regelung verwendete Wort „Datenanalyse“ durch das Wort „Datenauswertung“ ersetzt, was insbesondere der Klarstellung dienen sollte, dass keine Systeme zum Einsatz kommen, die über den Einsatz von intelligenten, möglicherweise selbstlernenden Algorithmen selbstständig inhaltliche Bewertungen vornehmen (Hamburgische Bürgerschaft AusschussDrucks 21/40, Anlage 1, S. 1). Zudem wurde eine spezielle Berichtspflicht des Hamburger Senats gegenüber der Bürgerschaft eingeführt (§ 75 Sätze 1 und 2 HmbPolDVG). 14

Die Freie und Hansestadt Hamburg hat bislang nach eigenem Bekunden keine Versuche unternommen, eine hessenDATA vergleichbare Plattform zu errichten (Hamburgische Bürgerschaft Drucks 22/1758, S. 1 f.). Auch nach Abschluss eines Rahmenvertrags zwischen dem Freistaat Bayern und dem Unternehmen Palantir, der es anderen Ländern erlaubt, das ausgewählte Produkt, eine verfahrensübergreifende Recherche- und Analyseplattform (VeRA), ohne Vergabeverfahren selbstständig abzurufen, hat Hamburg über deren Einführung bislang keine Entscheidung getroffen (Hamburgische Bürgerschaft Drucks 22/7701, S. 1 f.). 15

IV.

Die Beschwerdeführenden des Verfahrens 1 BvR 1547/19 haben ihre Verfassungsbeschwerde am 2. Juli 2019 erhoben und mit Schriftsätzen vom 10. Mai 2021 und vom 23. September 2022 ergänzt. Die Verfassungsbeschwerde im Verfahren 1 BvR 2634/20 ist am 20. November 2020 eingegangen und wurde durch Schriftsätze vom 21. Dezember 2020 und vom 5. September 2022 ergänzt. Nach teilweiser Rücknahme weiterer Rügen durch die Beschwerdeführenden und infolge der Abtrennungsbeschlüsse des Senats vom 8. November 2022 sind hier allein die Regelungen des § 25a HSOG und des § 49 HmbPolDVG Verfahrensgegenstände. 16

In beiden Verfahren rügen die Beschwerdeführenden mit ähnlichem Vorbringen, § 25a HSOG beziehungsweise § 49 HmbPolDVG griffen unverhältnismäßig in ihr Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Soweit auch personenbezogene Daten aus Wohnraum- oder Telekommunikationsüberwachung in die Datenanalyse oder -auswertung einbezogen würden, seien überdies das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG und das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG verletzt. Im Verfahren 1 BvR 1547/19 machen die Beschwerdeführenden zudem für den Fall einer Einbeziehung von durch Online-Durchsuchung erhobenen Daten eine Verletzung der durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützten Vertraulichkeit und Integrität informationstechnischer Systeme geltend. In beiden Verfassungsbeschwerden wird ferner vorgetragen, aufgrund von Mängeln der angegriffenen Regelungen und ihrer Begleitbestimmungen liege auch eine Verletzung des Grundrechts auf effektiven Rechtsschutz aus Art. 19 Abs. 4 GG vor. 17

Die Beschwerdeführenden sind der Ansicht, aus der besonderen Eingriffsintensität der Ermächtigungen zur Verarbeitung personenbezogener Daten mittels einer automatisierten Anwendung zur Datenanalyse oder -auswertung ergäben sich besondere Rechtfertigungsanforderungen. Den nach § 25a HSOG und § 49 HmbPolDVG möglichen Maßnahmen komme eine ganz andere Qualität zu als einer bloßen weiteren Nutzung personenbezogener Daten, für die der Grundsatz der hypothetischen Datenneuerhebung als Maßstab genüge. Die schärferen Anforderungen seien durch die angegriffenen Regelungen nicht erfüllt. 18

Die hinsichtlich der eingesetzten Methoden offene Ermächtigung zur verdeckten Datenverarbeitung ohne Begrenzung von Datenart und -umfang erlaube die Erstellung von Persönlichkeits- und Sozialprofilen. Aufgrund der technischen Entwicklung ergäben sich neue, eingriffsintensivere Möglichkeiten der Herstellung von Verknüpfungen und der Erzeugung neuer Informationen, wobei auch der Einsatz komplexer Algorithmen und lernfähiger Systeme in Betracht komme. Soweit personenbezogene Daten aus der Wohnraum- oder Telekommunikationsüberwachung oder aus einer Online-Durchsuchung einflössen, erhöhe sich wegen des Persönlichkeitsbezugs der Daten das Gewicht des Eingriffs. Die Begrenzung auf bestehende polizeiliche Datenbestände schränke den möglichen Zugriff nicht hinreichend ein, da solche Bestände unter relativ geringen Anforderungen erweitert werden könnten. Weil von der Datenanalyse oder -auswertung in großer Zahl Menschen erfasst seien, die hierfür keinen Anlass gegeben hätten, könnten die Maßnahmen enorme Streubreite haben. Ein besonderes Risiko ergebe sich insoweit aus dem Zugriff auf Daten aus polizeilichen Vorgangsverwaltungsdatenbanken. 19

Datenanalysen und -auswertungen nach den angegriffenen Regelungen müssten einem herausragenden öffentlichen Interesse dienen und dürften daher nur zum Schutz von besonders gewichtigen Rechtsgütern wie Leib, Leben oder Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes zugelassen werden. Für diese müsse eine mindestens konkretisierte Gefahr bestehen. Für Maß- 20

nahmen nach der ersten Alternative des § 25a Abs. 1 HSOG und des § 49 Abs. 1 HmbPolDVG sei aber keine insofern ausreichende Eingriffsschwelle geregelt. Der in Bezug genommene Straftatenkatalog des § 100a Abs. 2 StPO umfasse zudem Gefährdungstatbestände, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisierten und teilweise die Strafbarkeit erheblich vorverlagerten. Auch würden nicht durchgängig hinreichend gewichtige Rechtsgüter vorausgesetzt. Der nach § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG relevante Katalog des § 100a Abs. 2 StPO enthalte auch Straftaten, deren Schutzgüter nicht gewichtig genug seien, zumal der insoweit einschränkende § 100a Abs. 1 Satz 1 Nr. 2 StPO hier keine Anwendung finde.

Die Beschwerdeführenden sind zudem der Ansicht, dass den angegriffenen Regelungen keine ausreichenden Verfahrenssicherungen in Bezug auf Transparenz, Rechtsschutz und Kontrolle zur Seite gestellt seien. Insoweit beanstanden sie, dass die Regelungen weder Benachrichtigungspflichten noch ein Auskunftsrecht enthielten. Auch die gesetzlichen Vorgaben für die Aufsicht seien ungenügend. Angesichts der Eingriffsschwere sei ein Richtervorbehalt oder jedenfalls eine Ausweitung der Befugnisse der Datenschutzbehörde sowie eine vollständige Protokollierung erforderlich. Zudem fehlten eingrenzende Vorgaben zur Dauer der Maßnahme, zur Löschung und zur Anwendung der aus den Grundsätzen der Zweckbindung und -änderung resultierenden Beschränkungen. 21

Im Verfahren 1 BvR 2634/20 machen die Beschwerdeführenden zudem Ausführungen zu besonderen rechtsstaatlichen Herausforderungen der möglichen Verwendung komplexer Algorithmen und (teil-)autonomer Datenverarbeitungssysteme, bei deren Einsatz effektiver Rechtsschutz nur zu gewährleisten sei, wenn eine wirksame technische Vorab- und Dauerkontrolle durch eine unabhängige Instanz erfolge. Bei den nach § 49 HmbPolDVG möglichen komplexen Analysen seien außerdem Vorkehrungen zur Sicherung ihrer Mindestqualität erforderlich. 22

V.

Im Verfahren 1 BvR 1547/19 haben die Hessische Staatskanzlei und der Hessische Beauftragte für Datenschutz und Informationsfreiheit, im Verfahren 1 BvR 2634/20 die Behörde für Justiz und Verbraucherschutz der Freien und Hansestadt Hamburg und der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Stellung genommen. Der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit hat in beiden Verfahren Stellungnahmen abgegeben. 23

1. Die Hessische Staatskanzlei hält die Verfassungsbeschwerde im Verfahren 1 BvR 1547/19 bereits für unzulässig. Sie scheitere aus Gründen der Subsidiarität. Außerdem sei die Beschwerdebefugnis nicht ausreichend dargelegt. Die Beschwerdeführenden setzten sich nur unzureichend mit den bislang noch nicht geklärten Möglichkeiten der Auslegung des § 25a HSOG in Zusammenschau mit weiteren Normen auseinander. 24

Sie verfehlten die Substantiierungsanforderungen aber auch deshalb, weil sie von vornherein von einem zu hohen Eingriffsgewicht ausgingen. Die Datenanalyse sei auf den rechtmäßigen polizeilichen Datenbestand beschränkt. Es würden lediglich vorhandene Daten sowie die darin erfassten Verbindungen nachvollziehbar zusammengeführt und dargestellt. Da eine Erhebung durch die Polizei und eine Speicherung in ihren Datenbanken nach den gesetzlichen Vorgaben erfolgt sein müsse, sei auch nicht eine unbegrenzte Zahl von Personen betroffen, die noch nie anlassbezogen polizeilich erfasst worden seien. Die Integration von Daten aus öffentlich zugänglichen sozialen Netzwerken in das nicht an das Internet angeschlossene Analysesystem hessenDATA könne nur manuell unter Beachtung der datenschutzrechtlichen Bestimmungen vorgenommen werden. Es gehe nicht um umfassende Persönlichkeitsbilder und Sozialprofile, sondern allein um die Effektivierung und Beschleunigung der Datenverarbeitung innerhalb eines klar definierten Datenbestands. Ein datenschutzrechtliches Sonderregime sei für die Durchführung der Datenanalyse nach § 25a HSOG nicht erforderlich, da die verfassungsrechtlichen Vorgaben durch die anwendbaren sonstigen Regelungen umgesetzt würden; hiermit hätten sich die Beschwerdeführenden nicht vertieft auseinandergesetzt. 25

Mit § 25a HSOG werde kein flächendeckend verfügbares Instrument geschaffen. Die Befugnis dürfe nur in begründeten Einzelfällen und unter Berücksichtigung des allgemeinen Verhältnismäßigkeitsgebots in Anspruch genommen werden. Die Nutzung zur vorbeugenden Bekämpfung von Straftaten setze tatsächliche Anhaltspunkte für die potenzielle Begehung einer Straftat voraus. Dabei wirke sich die Notwendigkeit eines Verdachts von schweren Straftaten nach § 100a Abs. 2 StPO zusätzlich gefahrerhöhend aus. Die Anforderungen an die Gefahrenprognose sänken, je höherwertig das durch die Straftat zu schützende Rechtsgut sei, so dass in aller Regel jedenfalls ein Anfangsverdacht für die Erforderlichkeit einer Datenanalyse nach § 25a Abs. 1 HSOG genüge. Bei der zweiten Anwendungsalternative werde hinreichend bestimmt eine konkrete Gefahr für die benannten Schutzgüter verlangt. 26

Auch die Beanstandung der Regelungen zur Gewährleistung von Transparenz, Rechtsschutz und Kontrolle sei nicht hinreichend substantiiert. Die gesetzlichen Informations-, Benachrichtigungs- und Auskunftspflichten nach § 29 HSOG in Verbindung mit §§ 50 bis 52 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) fänden auf § 25a HSOG ebenso Anwendung wie die Protokollpflichten nach § 71 HDSIG sowie die Berichtigungs-, Lösch- und Verarbeitungseinschränkungspflichten nach § 27 HSOG in Verbindung mit §§ 53, 70 HDSIG. Demensprechend sei für hessenDATA ein Löschkonzept mit umfangreichen Löschroutinen entwickelt worden, dessen Inhalte im Rahmen vorab stattfindender Schulungen und durch Unterlagen vermittelt würden. Der von den Beschwerdeführenden angeführten Gefahr eines missbräuchlichen Zugriffs durch beliebige Polizistinnen und Polizisten werde mit den Vorgaben des Hessischen Datenschutz- und Informationsfreiheitsgesetzes – insbesondere zur Sicherheit der Datenverarbeitung, zur Durchführung der Datenschutz-Folgenabschätzung und zur vorherigen Konsultation des Hessischen 27

Datenschutzbeauftragten – begegnet. Es seien zudem nach § 65 HDSIG ein Verzeichnis von Verarbeitungstätigkeiten anzufertigen, und nach § 59 Abs. 1 Satz 1 und § 66 HDSIG seien Maßnahmen zur Gewährleistung eines – unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen – dem Risiko angemessenen Schutzniveaus zu treffen. In Abstimmung mit dem Hessischen Datenschutzbeauftragten seien für hessenDATA in einem die genannten Grundsätze berücksichtigenden Rechte- und Rollenkonzept Nutzerkreise und strenge Nutzungsbedingungen festgelegt worden. Danach könne lediglich ein beschränkter Benutzerkreis in sachlich zuständigen Organisationsbereichen nach entsprechender Schulung, Belehrung und Freischaltung innerhalb des jeweiligen Zuständigkeitsbereichs die Analyseplattform nutzen.

Eine wirksame Aufsicht sei gewährleistet. Dem Datenschutzbeauftragten kämen 28
über die in § 25a Abs. 3 Satz 2 HSOG vorgesehene Einbindung hinaus seine Rechte aus § 14 HDSIG zu, wozu etwa das Recht der Beanstandung, der Anordnung von Abhilfemaßnahmen oder der Warnung zähle. Damit korrespondiere die Verpflichtung öffentlicher Stellen nach § 14 Abs. 4 Satz 1 HDSIG, den Datenschutzbeauftragten bei seinen Aufgaben zu unterstützen, was sich vor allem in der Pflicht zur Kooperation bei Ausübung der ihm zugewiesenen Untersuchungsbefugnisse – auch in Hinblick auf Verarbeitungsvorgänge inklusive der hierzu verwendeten Software – manifestiere. In Ergänzung dazu verpflichte § 63 HDSIG zur proaktiven Zusammenarbeit mit dem Hessischen Datenschutzbeauftragten; § 64 HDSIG sehe zudem bei Inbetriebnahme neuer Verarbeitungsvorgänge und bei wesentlichen Veränderungen bestehender Dateisysteme mit erheblichem Gefährdungspotenzial die Pflicht der für den Datenschutz verantwortlichen Stelle vor, sich an den Hessischen Datenschutzbeauftragten zu wenden und diesen anzuhören.

2. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit berichtet 29
über Schlussfolgerungen, die er vor dem Hintergrund seiner Prüftätigkeit im Hinblick auf die praktische Anwendung von hessenDATA gezogen habe, und gelangt zu der Einschätzung, § 25a HSOG sei verfassungswidrig.

Die Eingriffsschwellen seien gemessen am Eingriffsgewicht nicht bestimmt genug 30
beziehungsweise zu weit gefasst. Die beiden tatbestandlichen Alternativen bereiteten Schwierigkeiten bei der Definition eines klaren Anwendungsbereichs. Da die erste Alternative der vorbeugenden Bekämpfung von Straftaten die Anwendung weit ins Gefahrenvorfeld ziehe, in dem die Grenzen von Gefahrenabwehr und Strafverfolgung verschwömmen, drohe eine Umgehung der Strafprozessordnung, in der eine vergleichbare Rechtsgrundlage fehle. Es bestehe die Möglichkeit, dass der für die Weiterverarbeitung personenbezogener Daten erforderliche Ermittlungsansatz schon in den tatsächlichen Anhaltspunkten für das Vorliegen einer Straftat oder im Anfangsverdacht für eine Straftat nach § 100a Abs. 2 StPO gesehen und damit bereits eine Nutzung der Anwendung zu präventiven Zwecken begründet werde.

Wegen der Eingriffstiefe des sogenannten „Data-Mining“ sei die Eingriffsschwelle des § 25a Abs. 1 Alt. 1 HSOG nicht hinreichend qualifiziert. Zu fordern sei eine hinreichend konkretisierte Gefahr. Zu einer Einhegung der Anwendungsfälle im Gefahrenvorfeld tauge auch das Tatbestandsmerkmal „begründeter Einzelfall“ nicht, weil § 25a Abs. 1 Alt. 1 HSOG hierzu keine weiteren Anhaltspunkte enthalte und sich auch aus den gesetzlichen Protokollierungspflichten keine weitere Konturierung ergebe; entsprechend werde hessenDATA von den Behörden so genutzt, dass nicht an einen konkreten Sachverhalt in einem einzelnen Ermittlungsverfahren angeknüpft werde, sondern die Software in übergreifenden Vorgängen und Projekten in verschiedenen Phänomenbereichen Anwendung finde. Um eine wirkliche Auseinandersetzung im Einzelfall sowie eine rechtliche Überprüfung zu gewährleisten, sollte daher in § 25a HSOG im Sinne der Normenklarheit und Bestimmtheit eine gesonderte Pflicht zu einer ausformulierten und dokumentierten Begründung festgeschrieben werden. Die nach § 71 Abs. 2 HDSIG geforderte Begründung im Rahmen der Protokollierung genüge nicht, weil durch diese nur eine technische Nachvollziehbarkeit der Abfragen sichergestellt werde. 31

Eine erhöhte Eingriffsintensität ergebe sich aus der Vielzahl, Breite und Art der verwendeten Datenbestände, die auch Daten von Nichtstörern beziehungsweise Nichttatverdächtigen, strafprozessual millionenfach erhobene Daten (überwiegend unbeteiligter Personen) aus Funkzellenabfragen und polizeiexterne Daten umfassten. Nicht mehr angemessen erscheine § 25a HSOG ferner deswegen, weil mit der in Hessen eingesetzten Software Persönlichkeitsprofile erstellt werden könnten. Diese Gefahr bestehe insbesondere, weil nach § 20 Abs. 9 HSOG die Einbeziehung der umfangreichen, auch „sonstige Personen“ betreffenden Daten aus dem Vorgangsbearbeitungssystem ComVor als Durchbrechung der strengen Zweckbindung zulässig sei. Trotz des Rückgriffs auf solche Daten sowie der Komplexität der Analyse fehle es der Norm zudem an einer gesetzlichen Eingrenzung der Zugriffsmöglichkeiten und Nutzungen von Anwendungen wie hessenDATA. Zwar bestünden abgestufte Zugriffsrechte und Beschränkungen für Daten aus besonders eingriffsintensiven Maßnahmen, grundsätzlich könnten aber ohne konkrete gesetzliche Begrenzungen alle Nutzer zugreifen. 32

Betroffenenrechte und Rechtsschutzmöglichkeiten seien nicht hinreichend verankert. Problematisch sei, dass das gesetzliche Auskunftsrecht allein hinsichtlich der Quellsysteme und nicht auch hinsichtlich der Analyseergebnisse verstanden werden könne. Die Norm mache auch keine Vorgaben, wie eine Speicherfrist für die Analyseergebnisse umgesetzt werden solle. Auch spezielle gesetzliche Protokollierungspflichten nach § 28 HSOG oder die gesetzliche Benachrichtigungspflicht nach § 29 Abs. 5 in Verbindung mit § 28 Abs. 2 HSOG umfassten § 25a HSOG nicht, weswegen für eine betroffene Person bei Ablehnung eines Auskunftsersuchens zu § 25a HSOG Rechtsschutz kaum erreichbar sei. Schließlich seien die verfahrensbegleitenden Schutzmaßnahmen gemessen an der Eingriffsintensität unzureichend. Die Datenschutzbehörde sei lediglich 2019 mehrfach zu generellen phänomenbezogenen 33

Anordnungen der Polizeibehörden angehört worden, auf deren Grundlage die Anwendung von hessenDATA nunmehr offenbar solange erfolge, wie keine größeren Veränderungen in technischer Hinsicht beziehungsweise bei der Nutzung von Quellsystemen einträten. Dadurch laufe die als Absicherung in datenschutzrechtlicher Hinsicht gedachte Anhörung nach § 25a Abs. 3 Satz 2 HSOG leer. Hinzu komme, dass die Datenschutzbehörde nicht befugt sei, eine vorübergehende oder endgültige Beschränkung der Verarbeitung anzuordnen.

3. Die Behörde für Justiz und Verbraucherschutz der Freien und Hansestadt Hamburg zweifelt im Verfahren 1 BvR 2634/20 bereits an der Zulässigkeit der Verfassungsbeschwerde. Diese sei auch unbegründet. § 49 HmbPolDVG sei nur Ermächtigung für eine technische Hilfestellung für die im Einzelfall tätigen Polizisten und von allenfalls moderater Eingriffsqualität. Die Datenverarbeitung im Wege einer automatisierten Anwendung begründe keine andere Qualität, wegen der über die Grundsätze der hypothetischen Datenneuerhebung hinaus weitere Anforderungen angelegt werden müssten. Der automatisierte Zugriff unterscheide sich nicht vom gezielten Blick eines Beamten in eine Akte oder ein Dateisystem im Sinne einer manuellen Auswertung; für diese werde lediglich ergänzend eine technische Alternative bereitgestellt. Insbesondere gehe es trotz der Beschreibung in Absatz 2 nicht darum, gewissermaßen anlassunabhängig umfassende Sozialprofile ganzer Milieus oder Persönlichkeitsprofile zu erstellen. Zum einen komme dem Merkmal „in begründeten Einzelfällen“ deutlich einschränkende Wirkung zu, zum anderen unterliege auch die weitere Behandlung der durch die Anwendung gewonnenen Erkenntnisse den gesetzlichen Vorgaben des Datenschutzrechts. 34

Bedeutsam sei zudem, dass § 49 HmbPolDVG nicht zu Datenerhebungen ermächtige, die Möglichkeiten einer Gewinnung neuer Erkenntnisse also durch den vorhandenen Datenbestand eingeschränkt seien. Dass sich so neue Verdachtsmomente ergeben könnten, an die sich operative Maßnahmen anschließen, sei bei der Verarbeitung von in polizeilichen Dateisystemen gespeicherten Daten nichts Ungewöhnliches. Die angegriffene Regelung sei den Vorstellungen des Gesetzgebers gemäß auszulegen, der den Einsatz von Software zum „predictive policing“ abgelehnt habe und den Einsatz komplexer Algorithmen und lernfähiger Systeme nicht zulassen wollte. Dies komme auch in der Ersetzung des Begriffs „Datenanalyse“ durch „Datenauswertung“ zum Ausdruck. 35

Die erste tatbestandliche Alternative der vorbeugenden Bekämpfung bestimmter Straftaten umfasse lediglich die „Verhütung von Straftaten“, nicht aber die „Vorsorge für die Verfolgung künftiger Straftaten“. Angesichts des Wortlauts der angegriffenen Regelung, insbesondere des Merkmals „in begründeten Einzelfällen“, seien zudem stets tatsächliche Anhaltspunkte für die bevorstehende Begehung einer Straftat zu fordern; eine abstrakte Gefahrenlage genüge nicht. Bereits die tatbestandliche Anknüpfung an bestimmte Straftatbestände verlange zwangsläufig hinreichende und gesicherte Erkenntnisse über den erwarteten Geschehensablauf. Es sei auch nicht zu beanstanden, dass die angegriffene Regelung für die einzusetzende automatisier- 36

te Anwendung zur Datenauswertung keine konkreten Vorgaben mache. Der Gesetzgeber dürfe Ermächtigungsgrundlagen grundsätzlich technikoffen halten. Detailliertere Verfahrensregelungen seien angesichts der nicht besonders hohen Eingriffsintensität der Norm, die bereits durch eine Vielzahl von Verfahrensbestimmungen des gesetzlichen Gesamtkontexts flankiert sei, nicht erforderlich.

4. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit teilt im Ergebnis weithin die Bedenken der Beschwerdeführenden im Verfahren 1 BvR 2634/20. 37

§ 49 HmbPolDVG schaffe kaum begrenzte Möglichkeiten der Zusammenführung zur Weiternutzung vormals getrennter, zweckgebundener polizeilicher Daten. Besonders kritisch sei, dass auch die polizeilichen Vorgangsverwaltungs- und Bearbeitungssysteme einbezogen werden könnten. Diese dienten dem Auffinden von Vorgängen und der Rekonstruktion, welche Anzeigen, Sachverhalte und sonstigen Geschehnisse im Zuge der polizeilichen Tätigkeit bearbeitet worden seien. In diese Datenbanken werde eine nicht unerhebliche Zahl von Betroffenen ohne eigenes Zutun aufgenommen. 38

Auch die an § 6a ATDG angelehnte Regelung der Methode wirke eingriffsverstärkend. Die im Gesetzgebungsverfahren geäußerte Ansicht, mit der Ersetzung des Begriffs der „Datenanalyse“ durch den der „Datenauswertung“ sei ein „Data-Mining“ ausgeschlossen, überzeuge kaum. Welche Methodik zur Verarbeitung verwendet werden solle, sei in § 49 HmbPolDVG nicht ersichtlich; die Gesetzesentstehung lasse erkennen, dass es um Effektivitätssteigerungen gehe. Es bestehe das Risiko der Erzeugung nahezu umfassender Persönlichkeitsbilder und Sozialprofile verdächtiger Zielpersonen; die Verarbeitung verschaffe der Polizei neue Erkenntnisse und Zusammenhänge. 39

Die in der angegriffenen Regelung formulierte Voraussetzung „in begründeten Einzelfällen…erforderlich“ genüge nicht den verfassungsrechtlichen Anforderungen an die Eingriffsschwelle, wonach wenigstens tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr zu verlangen seien. Fraglich sei, ob angesichts der Eingriffsschwere die Mindestschwelle einer konkreten Gefahr überhaupt noch genüge. Höher müsse die Eingriffsschwelle jedenfalls liegen, wenn Daten verarbeitet würden, die aus einer Wohnraumüberwachung erlangt wurden. Eine entsprechende polizeiliche Praxis sei zwar angesichts der allgemeinen Grundsätze der Zweckbindung für die Weiterverwendung von Daten nach § 34 Abs. 4 HmbPolDVG möglich, jedoch praktisch wegen der potenziellen Menge an Abfragen problematisch. In jedem Fall wäre eine solche Lösung technisch anspruchsvoll, weil im Rahmen der Zusammenführung verschiedene Eingriffsschwellen für unterschiedliche Dateisysteme abgebildet werden müssten. 40

Auch sei zum Teil sehr zweifelhaft, ob mit dem in Bezug genommenen Katalog des § 100a Abs. 2 StPO hinreichend bedeutsame Rechtsgüter geschützt würden. Außerdem bedürfe es einer speziellen Auskunftsregelung und spezieller Löschpflichten. 41

Zudem müsse die aufsichtsrechtliche Kontrolle erweitert werden, da nach gegenwärtiger Gesetzeslage eine sinnvolle Aufsicht durch die Datenschutzbehörde nicht möglich sei.

5. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zweifelt an der Verfassungsmäßigkeit des § 25a HSOG und des § 49 HmbPolDVG. 42

Den Regelungen komme eine erhöhte Eingriffsintensität zu, weil auf ihrer Grundlage ein umfassender Zugriff auf sämtliche polizeiliche Datenbestände und damit potenziell auf eine sehr große Menge teils sensibler Daten eines großen Kreises von Personen genommen werden könne. Problematisch seien insbesondere die Einbeziehung von Vorgangsbearbeitungssystemen und die perspektivischen Möglichkeiten einer umfassenden Einbeziehung der Datenbanken anderer Polizeien von Bund und Ländern. Weiterhin erhöhe die Art und Weise der Datenverarbeitung das Eingriffsgewicht. Das durch die Regelungen zugelassene „Data-Mining“ gehe über die Rasterfahndung hinaus, weil diese immer noch durch ein begrenzendes Auswerteraster geprägt sei, nun aber Systeme Daten auch unabhängig von einem Raster mit trainierten oder selbstlernenden Algorithmen auswerteten. Eine Nutzung von künstlicher Intelligenz sei nicht ausgeschlossen. Problematisch sei dabei unter Transparenzgesichtspunkten, dass beim maschinellen Lernen nach dem derzeitigen Stand der Technik die Nachvollziehbarkeit nicht sichergestellt sei. 43

Das unklare Merkmal „begründeter Einzelfall“ werde weder durch das Erfordernis einer konkreten Gefahrenlage oder tatsächlicher Anhaltspunkte noch durch eine sonstige Schwelle eingegrenzt, so dass in der polizeilichen Praxis eine sehr weite Auslegung zu befürchten sei. Es drohe eine Anwendung bereits bei bestimmten Entwicklungen einer polizeilichen Lage (etwa allgemeine Zunahme von Drogendelikten) oder bei jeder Strafanzeige. Die Vorschriften könnten zum Standardinstrument werden. Auch der Verweis auf § 100a Abs. 2 StPO sei problematisch, unter anderem weil der Katalog nach den Erweiterungen der letzten Jahre auch niederschwellige Delikte aufliste. 44

Zudem sei zweifelhaft, ob die notwendige Trennung nach den unterschiedlichen Zweckbestimmungen bei der automatisierten Datenauswertung praktisch gewährleistet werden könne. Die Einhaltung der Zweckbindung sei bei Zusammenführung und Abgleich einer großen Menge von Daten aus unterschiedlichen Quellen schwierig. Eine Durchbrechung der Zweckbindung sei zwar für § 49 HmbPolDVG anders als bei § 25a in Verbindung mit § 20 Abs. 9 Satz 3 HSOG nicht ausdrücklich geregelt, aber der Zielrichtung nach offenbar auch dort intendiert. 45

VI.

Das Bundesverfassungsgericht hat am 20. Dezember 2022 eine mündliche Verhandlung durchgeführt. Geäußert haben sich die Beschwerdeführenden, die Hessische Landesregierung sowie der Senat der Freien und Hansestadt Hamburg. Als sachkundige Dritte nach § 27a BVerfGG haben sich der Hessische Beauftragte für 46

Datenschutz und Informationsfreiheit, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie Dr. Constanze Kurz für den Chaos Computer Club e.V. geäußert.

B.

Die Verfassungsbeschwerden gegen § 25a HSOG und gegen § 49 HmbPolDVG sind zulässig, soweit sie gegen die Eingriffsschwelle in § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG (Datenanalyse oder -auswertung zur vorbeugenden Bekämpfung von Straftaten) gerichtet sind. Insoweit erscheint eine Verletzung der Beschwerdeführenden in ihrer durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG als Ausprägung des allgemeinen Persönlichkeitsrechts geschützten informationellen Selbstbestimmung möglich. 47

Im Übrigen sind die Verfassungsbeschwerden unzulässig. Gegenstand der Prüfung ist damit weder die Frage, ob die Gesetzgeber verfassungsrechtlich ausreichende Regelungen zu den durch die Datenanalyse oder -auswertung nach § 25a HSOG und § 49 HmbPolDVG zu schützenden Rechtsgütern getroffen haben. Noch ist hier zu überprüfen, ob die für Transparenz und Rechtsschutz sorgenden Verfahrens- und Organisationsregelungen verfassungsrechtlichen Anforderungen genügen, ob insbesondere auch mit Blick auf komplexe Formen automatisierten Datenabgleichs bis hin zu selbstlernenden Systemen (Künstliche Intelligenz, „KI“) hinreichende verfahrensrechtliche Sicherungen bestehen. Es ist auch nicht zu prüfen, ob der verfassungsrechtliche Grundsatz der Zweckbindung bereits erhobener personenbezogener Daten gewahrt ist, ob also insbesondere auch hinreichend begrenzt ist, inwiefern Daten, die unter Eingriff in Art. 13 Abs. 1 GG oder Art. 10 Abs. 1 GG erhoben worden sind, weiter genutzt werden dürfen. Insoweit haben die Beschwerdeführenden die Möglichkeit einer Grundrechtsverletzung nicht ausreichend dargelegt. Überwiegend fehlen konkretere Ausführungen zu den verfassungsrechtlichen Anforderungen. Zudem hätte eine nähere Auseinandersetzung mit dem einfachgesetzlichen Normenbestand erfolgen müssen, vor allem mit der Frage, warum die aus Sicht der Beschwerdeführenden gebotenen Sicherungen nicht bereits in anderen Bestimmungen des geltenden Rechts, insbesondere des Landesdatenschutz- und Polizeirechts, enthalten sind, die konkret zu benennen und deren Reichweite zu erörtern gewesen wären (vgl. dazu auch BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 129, 132 – Bayerisches Verfassungsschutzgesetz). 48

C.

Die Verfassungsbeschwerden sind, soweit sie zulässig sind, begründet. Aufgrund der angegriffenen Befugnis kann jedenfalls in die durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG als Ausprägung des allgemeinen Persönlichkeitsrechts geschützte informationelle Selbstbestimmung eingegriffen werden (I). Ein Grundrechtseingriff durch automatisierte Datenanalyse oder -auswertung durch Polizeibehörden 49

ist grundsätzlich verfassungsrechtlich rechtfertigbar. Die verfassungsrechtlichen Anforderungen an die Rechtfertigung einer automatisierten Datenanalyse oder -auswertung richten sich nach der konkreten Reichweite der Befugnis und sind entsprechend variabel; hier sind sie angesichts der Ausgestaltung der angegriffenen Vorschriften streng (II). § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG enthalten danach keine ausreichende Eingriffsschwelle (III). Beide Vorschriften sind deshalb verfassungswidrig. Dies betrifft die Datenanalyse oder -auswertungsbefugnis zur vorbeugenden Straftatenbekämpfung. Die Befugnis zur Abwehr von Gefahren (§ 25a Abs. 1 Alt. 2 HSOG, § 49 Abs. 1 Alt. 2 HmbPolDVG) bleibt unberührt.

I.

Werden gespeicherte Datenbestände gemäß § 25a HSOG oder § 49 HmbPolDVG mittels einer automatisierten Anwendung zur Datenanalyse oder -auswertung verarbeitet, greift dies in die informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) aller ein, deren Daten bei diesem Vorgang personenbezogen Verwendung finden. Mit der automatisierten Auswertung gespeicherter Daten erlaubt der Gesetzgeber eine weitere Nutzung früher erhobener Daten über den ursprünglichen Anlass hinaus. Das begründet einen neuen Grundrechtseingriff und muss verfassungsrechtlich eigens nach dem Grundsatz der Zweckbindung gerechtfertigt werden (vgl. BVerfGE 141, 220 <324 Rn. 277, 327 Rn. 285>; näher unten Rn. 55 ff.). Indessen liegt ein Grundrechtseingriff hier nicht nur in der weiteren, zusammenführenden Verwendung vormals getrennter Daten, sondern darüber hinaus in der Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die automatisierte Datenanalyse oder -auswertung geschaffen werden kann (vgl. BVerfGE 156, 11 <39 f. Rn. 73 f.>; näher unten Rn. 67 ff.). 50

II.

Die Rechtfertigung eines Grundrechtseingriffs setzt eine gesetzliche Ermächtigung voraus, die einen legitimen Zweck verfolgt und auch im Übrigen dem Grundsatz der Verhältnismäßigkeit genügt. 51

Die angegriffenen Regelungen dienen dem legitimen Zweck, vor dem Hintergrund informationstechnischer Entwicklung die Wirksamkeit der vorbeugenden Bekämpfung schwerer Straftaten zu steigern, indem Anhaltspunkte für bevorstehende schwere Straftaten gewonnen werden, die im Datenbestand der Polizei ansonsten unerkannt blieben. Die hessische Landesregierung hat in diesem Verfahren dargelegt, die Polizeibehörden seien infolge der insbesondere in den Bereichen terroristischer und extremistischer Gewalt sowie der organisierten und schweren Kriminalität zunehmenden Nutzung digitaler Medien und Kommunikationsmittel mit einem ständig anwachsenden und nach Qualität und Format zunehmend heterogenen Datenaufkommen konfrontiert. Die dazu in den polizeilichen Datenbeständen enthaltenen Informationen könnten gerade unter Zeitdruck kaum manuell gewonnen werden; eine automatisierte Datenanalyse sei daher von großer Bedeutung für erfolgreiches 52

polizeiliches Handeln.

Zur Steigerung der Wirksamkeit vorbeugender Straftatenbekämpfung sind die Regelungen im verfassungsrechtlichen Sinne geeignet. Sie sind auch erforderlich, weil durch eine automatisierte Datenanalyse oder -auswertung für die Verhütung von Straftaten relevante Erkenntnisse erschlossen werden können, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu gewinnen wären. 53

Spezielle Anforderungen ergeben sich hier aus dem Gebot der Verhältnismäßigkeit im engeren Sinne. Wie streng diese Anforderungen im Einzelnen sind, bestimmt sich nach dem Eingriffsgewicht der Maßnahme (vgl. BVerfGE 141, 220 <269 Rn. 105>; 155, 119 <178 Rn. 128> – Bestandsdatenauskunft II; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 152; stRspr). Das Eingriffsgewicht einer automatisierten Datenanalyse oder -auswertung und die verfassungsrechtlichen Rechtfertigungsanforderungen ergeben sich zum einen aus dem Gewicht der vorausgegangenen Datenerhebungseingriffe; insoweit gelten die Grundsätze der Zweckbindung und Zweckänderung (1). Zum anderen hat die automatisierte Datenanalyse oder -auswertung potenziell ein Eigengewicht, so dass weitergehende Rechtfertigungsanforderungen gelten (2). 54

1. Nach § 25a HSOG und § 49 HmbPolDVG werden im Wege der automatisierten Datenanalyse oder -auswertung personenbezogene Daten weiterverarbeitet, die bereits früher erhoben und gespeichert worden sind. Die Rechtfertigungsanforderungen an die weitere Nutzung staatlich erhobener Daten richten sich nach den Grundsätzen der Zweckbindung und Zweckänderung (grundlegend BVerfGE 65, 1 <46>). Erlaubt der Gesetzgeber die Nutzung von Daten über den konkreten Anlass und rechtfertigenden Grund einer Datenerhebung hinaus, muss er hierfür eine eigene Rechtsgrundlage schaffen. Er kann unter Wahrung der näheren verfassungsrechtlichen Anforderungen sowohl eine weitere Nutzung der Daten im Rahmen der für die Datenerhebung maßgeblichen Zwecke vorsehen (a) als auch eine Zweckänderung erlauben (b) (vgl. BVerfGE 141, 220 <324 ff. Rn. 276 ff.> m.w.N.; stRspr). § 25a HSOG und § 49 HmbPolDVG erlauben sowohl zweckwahrende als auch zweckändernde Weiternutzungen (c). 55

a) Der Gesetzgeber kann zum einen eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus als weitere Nutzung im Rahmen der ursprünglichen Zwecke dieser Daten erlauben; er unterliegt dann den im Urteil zum Bundeskriminalamtgesetz näher konturierten verfassungsrechtlichen Anforderungen an die zweckwahrende Weiternutzung (vgl. BVerfGE 141, 220 <324 ff. Rn. 278 ff.> m.w.N.). 56

Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt die zur Datenerhebung ermächtigte Behörde, den Zweck und die Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an 57

bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich: Ist diese nur zum Schutz bestimmter Rechtsgüter oder zur Verhütung bestimmter Straftaten erlaubt, so begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine Zweckänderung eine weitergehende Nutzung erlaubt.

Nicht zu den Zweckbindungen, die für jede weitere Nutzung der Daten seitens derselben Behörde im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten je neu beachtet werden müssen, gehören grundsätzlich die für die Datenerhebung maßgeblichen Anforderungen an Eingriffsschwellen, wie sie traditionell die hinreichend konkretisierte Gefahrenlage im Bereich der Gefahrenabwehr und ein qualifizierter Tatverdacht im Bereich der Strafverfolgung darstellen. Das Erfordernis einer hinreichend konkretisierten Gefahrenlage oder eines qualifizierten Tatverdachts bestimmt den Anlass, aus dem entsprechende Daten erhoben werden dürfen, nicht aber die erlaubten Zwecke, für die die Daten der Behörde dann zur Nutzung offenstehen. Folglich widerspricht es nicht von vornherein dem Gebot einer dem ursprünglichen Erhebungszweck entsprechenden Verwendung, wenn die weitere Nutzung solcher Daten bei Wahrnehmung derselben Aufgabe auch unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz erlaubt wird. Die Behörde kann die insoweit gewonnenen Kenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung – allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen – als schlichten Ausgangspunkt für weitere Ermittlungen nutzen. Damit ist keine Datennutzung ins Blaue hinein eröffnet. Vielmehr hat auch eine Verwendung der Daten als Spurenansatz durch die Bindung an die für die Datenerhebung maßgeblichen Aufgaben und die Anforderungen des Rechtsgüterschutzes einen hinreichend konkreten Ermittlungsbezug. Für die Wahrung der Zweckbindung kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt. Diese Anforderungen sind erforderlich, aber grundsätzlich auch ausreichend, um eine weitere Nutzung der Daten im Rahmen der Zweckbindung zu legitimieren. 58

Weiter reicht die Zweckbindung allerdings für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen: Hier ist jede weitere Nutzung der Daten, auch seitens derselben Behörde im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten, nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr (vgl. dazu BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 297 m.w.N.) oder im Einzelfall zumindest hinreichend konkreti- 59

sierten Gefahr (vgl. dazu BVerfGE 141, 220 <272 f. Rn. 112>) erforderlich ist. Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall hinreichend konkretisierten Gefahr kommt hier nicht in Betracht.

b) Der Gesetzgeber kann zum anderen eine weitere Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung); als Ermächtigung zu einer Datennutzung für neue Zwecke unterliegt sie den im Urteil zum Bundeskriminalamtgesetz formulierten verfassungsrechtlichen Anforderungen an die zweckändernde Weiternutzung von Daten (vgl. BVerfGE 141, 220 <326 ff. Rn. 284 ff.> m.w.N.). 60

Die Ermächtigung zu einer Nutzung von Daten zu neuen Zwecken begründet einen neuen Eingriff in das Grundrecht, in das durch die Datenerhebung eingegriffen wurde. Zweckänderungen sind folglich jeweils an den Grundrechten zu messen, die für die Datenerhebung maßgeblich waren. Hierbei orientiert sich das Gewicht, das einer solchen Regelung im Rahmen der Abwägung zukommt, am Gewicht des Eingriffs der Datenerhebung. Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, können auch nur zu besonders gewichtigen Zwecken genutzt werden. Als Maßstab der Verhältnismäßigkeitsprüfung gilt insoweit das Kriterium der hypothetischen Datenneuerhebung. 61

Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben werden dürften. Voraussetzung für eine Zweckänderung ist danach, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrads der Gefahrenlage oder des Tatverdachts, also hinsichtlich der Eingriffsschwelle. Die diesbezüglichen Anforderungen bestimmen unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst, nicht aber auch für die weitere Nutzung der erhobenen Daten. Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt. 62

Der Gesetzgeber kann danach – bezogen auf die Datennutzung von Sicherheitsbe- 63

hörden – eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist.

Anderes gilt allerdings wie bei der zweckwahrenden Weiterverarbeitung auch hier für Informationen aus Wohnraumüberwachungen oder dem Zugriff auf informationstechnische Systeme. Angesichts des besonderen Eingriffsgewichts dieser Maßnahmen muss hier jede neue Nutzung der Daten wie bei der Datenerhebung selbst auch durch eine dringende Gefahr oder eine im Einzelfall hinreichend konkretisierte Gefahr gerechtfertigt sein. 64

c) Nach § 25a HSOG und § 49 HmbPolDVG können personenbezogene Daten sowohl zweckwahrend als auch zweckändernd weiterverarbeitet werden. Die beiden Vorschriften erlauben die Verarbeitung sehr großer Datenmengen, im Wesentlichen ohne selbst nach der Herkunft der Daten und den ursprünglichen Erhebungszwecken zu unterscheiden. Zur Wahrung der verfassungsrechtlichen Anforderungen der Zweckbindung müssten darum anderweitig hinreichend normenklare Regelungen getroffen sein, die die Einhaltung des Grundsatzes der Zweckbindung rechtlich und praktisch sichern. Materiell ist bei der fachrechtlichen Ausgestaltung der Zweckbindung auch zu beachten, dass eine Datenanalyse oder -auswertung von Daten, die zwar gegenwärtig in den eigenen Datenbeständen der Behörde gespeichert sind, die aber ursprünglich von einer anderen Stelle erhoben und an sie weitergegeben wurden, keine weitere Nutzung im Rahmen der ursprünglichen Zwecke sein kann, sondern schon wegen dieses Behördenwechsels als zweckändernde Datennutzung den dafür geltenden verfassungsrechtlichen Anforderungen unterliegt. Entsprechend wurde etwa in der mündlichen Verhandlung seitens des Hessischen Ministeriums des Innern und für Sport bekundet, dass unter den Voraussetzungen des § 479 Abs. 2 Satz 2 Nr. 2 StPO in eine Datei der hessischen Polizei gelangte Daten auch später nur unter den Voraussetzungen dieser Vorschrift gemäß § 25a HSOG erneut verarbeitet werden dürfen. Praktisch dürfte zur Einhaltung des verfassungsrechtlichen Zweckbindungsgrundsatzes insbesondere eine Kennzeichnung von Daten erforderlich sein (vgl. etwa § 20a HSOG und § 65 HmbPolDVG; s. aber zur Befreiung hiervon § 20a Abs. 4 HSOG und § 78 Abs. 1 HmbPolDVG; s. auch § 91 BKAG). Ob diese verfassungsrechtlichen Anforderungen hier eingehalten sind, muss allerdings offen bleiben, da dies von den Beschwerdeführenden nicht zulässig gerügt worden ist (oben Rn. 48). 65

2. Ob der Grundrechtseingriff verfassungsrechtlich gerechtfertigt ist, lässt sich aber bei einer Datenanalyse oder -auswertung nicht allein mit Blick auf das Gewicht der ursprünglichen Datenerhebung beurteilen, weil die weitere Verarbeitung durch eine automatisierte Datenanalyse oder -auswertung eigene Belastungseffekte haben kann, die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen (a). Das spezifische Eingriffsgewicht einer automatisierten Datenanalyse oder -auswer- 66

tung ist nicht immer gleich, sondern hängt von der näheren Ausgestaltung dieser Befugnis ab. Anhand genereller Maßstäbe lässt sich bestimmen, welchen verfassungsrechtlichen Anforderungen eine Befugnis zur automatisierten Datenanalyse oder -auswertung je nach Ausgestaltung unterliegt (b). Die konkreten Rechtfertigungsanforderungen hängen dann davon ab, wie der Gesetzgeber die Befugnis im Einzelnen regelt; hier sind die Rechtfertigungsanforderungen wegen der potenziellen Reichweite von § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG hoch (c).

a) Eine weitere Bearbeitung von einmal erhobenen und gespeicherten Daten durch eine automatisierte Datenanalyse oder -auswertung kann spezifische Belastungseffekte haben, die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen (vgl. BVerfGE 156, 11 <39 Rn. 73>). Die automatisierte Datenanalyse oder -auswertung nach § 25a HSOG und § 49 HmbPolDVG ist darauf gerichtet, neues Wissen zu erzeugen. § 25a Abs. 2 HSOG und § 49 Abs. 2 HmbPolDVG beschreiben dies als das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen, den Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten. Rechtlich kann die handelnde Behörde aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen sowie aus der Auswertung neue Zusammenhänge erschließen. Die Verknüpfung von Daten ermöglicht etwa mehrstufige Analysen, die neue Verdachtsmomente erst erzeugen, sowie weitere Analyseschritte oder auch daran anschließende operative Maßnahmen (BVerfGE 156, 11 <40 Rn. 73>). 67

Zwar ist es für sich genommen nicht ungewöhnlich, dass die Polizei ihre einmal gewonnenen Erkenntnisse als Spuren- oder Ermittlungsansätze allein oder in Verknüpfung mit anderen ihr zur Verfügung stehenden Informationen als Ausgangspunkt weiterer Ermittlungen nutzt (vgl. BVerfGE 141, 220 <325 f. Rn. 281>). Auch die alltägliche polizeiliche Erkenntnisgewinnung ist Ergebnis einer Zusammenstellung und Bewertung von aus unterschiedlichen Quellen erlangten Informationen (vgl. Rademacher, AöR 142 <2017>, S. 366 <369, 372 ff.>; s. auch Schneider, GSZ 2020, S. 1 <4 f.>; Kuhlmann/Trute, GSZ 2021, S. 103 <104>). 68

Die automatisierte Analyse oder Auswertung nach § 25a HSOG und § 49 HmbPolDVG geht aber schon deshalb weiter, weil sie die Verarbeitung großer und komplexer Informationsbestände ermöglicht. Je nach der eingesetzten Analysemethode können zudem durch verknüpfende Auswertung vorhandener Daten neue persönlichkeitsrelevante Informationen gewonnen werden, die ansonsten so nicht zugänglich wären. Die Maßnahme erschließt die in den Daten enthaltenen Informationen damit intensiver als zuvor. Sie bringt nicht nur in den Daten angelegte, aber zunächst mangels Verknüpfung verborgene Erkenntnisse über Personen hervor, sondern kann sich bei entsprechendem Einsatz einem „Profiling“ (vgl. § 41 Nr. 4 HDSIG, § 2 Abs. 10 HmbPolDVG) annähern (vgl. Bäuerle, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, 27. Edition, Stand: 1. Oktober 2022, § 25a HSOG, Rn. 21 69

ff.). Denn es können sich softwaregestützt neue Möglichkeiten einer Vervollständigung des Bildes von einer Person ergeben, wenn Daten und algorithmisch errechnete Annahmen über Beziehungen und Zusammenhänge aus dem Umfeld der Betroffenen einbezogen werden. Insoweit kann auch die Kombination personenbezogener und nicht personenbezogener Daten und gegebenenfalls die algorithmentypische Berücksichtigung bloßer Korrelationen neue, sonst nicht sicht- oder ermittelbare persönlichkeitsrelevante Aufschlüsse geben. Ein herkömmliches Verfahren, die nach dem Modell abgestufter Erkenntnisverdichtung erfolgende Ermittlungstätigkeit, wird hierdurch mit einer viel größeren Durchschlagskraft versehen (vgl. BVerfGE 115, 320 <356 f.> m.w.N. – zur Rasterfahndung).

Regelmäßig sichert der Grundsatz der Zweckbindung die Verhältnismäßigkeit des in der Weiterverarbeitung bereits erhobener Daten liegenden Grundrechtseingriffs (oben Rn. 55 ff.). Dieser Grundsatz wurde jedoch vor dem Hintergrund einer im Wesentlichen manuellen Sichtung und Verknüpfung personenbezogener Daten näher konturiert, die in den tatsächlichen Kapazitätsgrenzen solcher Arbeitsweise auch ihre praktischen Erkenntnisgrenzen finden. Das Ziel einer Befugnis zur automatisierten Datenanalyse oder -auswertung ist nun aber gerade, diese praktischen Erkenntnisgrenzen zu überwinden. Das ist verfassungsrechtlich legitim, weil es der Effektuierung der Gefahrenbekämpfung dient. Mit der Überwindung der praktischen Erkenntnisgrenzen klassischer Polizeiarbeit gehen jedoch auch besondere Gefahren für die durch die Datenverarbeitung Betroffenen einher. Je nach Ausgestaltung kann die automatisierte Anwendung – insbesondere in Abhängigkeit von Art und Umfang der verarbeiteten Daten und von den Verarbeitungsmethoden – die Erstellung von Bewegungs- und Verhaltens- oder Beziehungsprofilen oder noch umfassenderer Persönlichkeitsbilder ermöglichen, die so im Wege händischer Suche oder einfacher automatisierter Abgleiche nicht erlangt werden könnten. Die automatisierte Anwendung kann die Arbeitsweise und Erkenntnismöglichkeiten der Polizei somit entscheidend verändern und kann so auch das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen (vgl. auch BVerfGE 156, 11 <39 f. Rn. 73> m.w.N.). Der verfassungsrechtliche Grundsatz der Zweckbindung könnte dem Eingriffsgewicht dann für sich genommen nicht hinreichend Rechnung tragen. 70

b) Die verfassungsrechtlichen Anforderungen an die Rechtfertigung einer automatisierten Datenanalyse oder -auswertung variieren (aa). Denn eine Besonderheit der Datenanalyse oder -auswertungsbefugnis liegt darin, dass die Eingriffsintensität der darauf gestützten Maßnahmen je nach gesetzlicher Ausgestaltung sehr unterschiedlich sein kann (bb). Entsprechend variabel sind die Anforderungen an die Eingriffsvoraussetzungen, also insbesondere an die Eingriffsschwelle, das zu schützende Rechtsgut und die Sicherung von Transparenz, Rechtsschutz und aufsichtlicher Kontrolle (cc), deren Regelung dem Grundsatz des Gesetzesvorbehalts, dem Gebot der Normenklarheit und dem Bestimmtheitsgebot genügen muss (dd). 71

aa) Die verfassungsrechtlichen Anforderungen an die Rechtfertigung einer automatisierten Datenanalyse oder -auswertung variieren, da deren Eingriffsintensität je 72

nach gesetzlicher Ausgestaltung ganz unterschiedlich sein kann. Bei einer Begrenzung der Befugnis auf eine sehr schlichte Form des Abgleichs einer überschaubaren Zahl von Daten näher eingegrenzter Herkunft ist das besondere Eigengewicht der Datenanalyse oder -auswertung gering. Je weiter die Möglichkeiten der automatisierten Weiterverarbeitung von Daten reichen, umso mehr entfernt sich der darin liegende Eingriff aber von der ursprünglichen Datenerhebung und umso weniger reicht der Grundsatz der Zweckbindung für sich genommen verfassungsrechtlich aus, um den erneuten Eingriff zu rechtfertigen.

Ermöglicht die automatisierte Datenanalyse oder -auswertung einen schweren Eingriff in die informationelle Selbstbestimmung der Betroffenen, lässt sie etwa die Erstellung von genaueren Bewegungs-, Verhaltens- oder Beziehungsprofilen zu oder setzt sie vermehrt Personen, die objektiv nicht zurechenbar in das relevante Geschehen verfangen sind, dem Risiko aus, aufgrund der Ergebnisse der automatisierten Datenanalyse oder -auswertung weiteren, gezielt gegen sie gerichteten, polizeilichen Ermittlungsmaßnahmen unterzogen zu werden, ist dies nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten (Rn. 104 ff.). 73

Sind hingegen die Möglichkeiten der Erkenntnisgewinnung so eingegrenzt, dass kein besonders schwerer eigenständiger Eingriff in die informationelle Selbstbestimmung der Betroffenen erfolgen kann, kann die Befugnis zur automatisierten Datenanalyse oder -auswertung an eine niedrigere Eingriffsschwelle geknüpft werden oder kann die Polizei davon auch zum Schutz von weniger gewichtigen Rechtsgütern Gebrauch machen (Rn. 107). Unter Umständen kann dann schon die Einhaltung des Grundsatzes der Zweckbindung zur verfassungsrechtlichen Rechtfertigung der weiteren Verarbeitung der Daten in einer automatisierten Anwendung ausreichen (näher unten Rn. 108). 74

bb) Wie streng die Anforderungen an die Eingriffsschwelle und den Rechtsgüterschutz bei einer Datenanalyse oder -auswertungsbefugnis im Einzelnen sind, bestimmt sich nach dem Eingriffsgewicht, das von verschiedenen Faktoren abhängt und demgemäß vom Gesetzgeber durch unterschiedliche Vorkehrungen und Kombinationen von Schutzmechanismen beeinflusst werden kann. 75

(1) Generell wird das Gewicht eines Eingriffs in die informationelle Selbstbestimmung vor allem durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt. Dabei ist unter anderem bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben. Maßgebend sind also die Gestaltung der Eingriffsschwellen, die Zahl der Betroffenen und die Intensität der individuellen Beeinträchtigung im Übrigen. Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträ- 76

gern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden. Dabei führt insbesondere die Heimlichkeit einer staatlichen Eingriffsmaßnahme ebenso zur Erhöhung ihrer Intensität wie die faktische Verwehrung vorherigen Rechtsschutzes und die Erschwerung nachträglichen Rechtsschutzes, wenn er überhaupt zu erlangen ist (BVerfGE 156, 11 <48 f. Rn. 96> m.w.N.; stRspr).

Das spezifische Eingriffsgewicht einer automatisierten Datenanalyse oder -auswertung hängt besonders davon ab, welcher Art das neue Wissen sein kann, das durch diese Maßnahmen erzeugt wird, insbesondere davon, ob und wie viel persönlichkeitsrelevantes Wissen so geschaffen wird. Das Eingriffsgewicht erhöht sich, wenn besonders private Informationen erlangt werden können. Besonders eingriffsintensiv ist auch, wenn sich das Verhalten einer Person, deren Gewohnheiten oder deren Lebensgestaltung räumlich und über längere Zeit hinweg nachvollziehen lassen, wenn also ein Bewegungs- oder Verhaltensprofil einer Person oder ein umfassenderes Persönlichkeitsbild entstehen kann (vgl. BVerfGE 115, 320 <350 f.>; 120, 378 <400 f., 406 f., 417>; 125, 260 <319 f.>; 141, 220 <267 Rn. 99>; 150, 244 <284 f. Rn. 100>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 287, 321 ff.; Beschluss des Ersten Senats vom 9. Dezember 2022 - 1 BvR 1345/21 -, Rn. 174 f. – Polizeiliche Befugnisse nach SOG MV). Das Eingriffsgewicht ist zudem höher, wenn die Polizei durch die Datenanalyse oder -auswertung Informationen über Personen erlangt und zum Ausgangspunkt weiterer operativer Maßnahmen macht, die objektiv in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den polizeilichen Eingriff durch ihr Verhalten nicht zurechenbar veranlasst haben (vgl. dazu BVerfGE 115, 320 <354 f.>; 150, 244 <283 Rn. 98>), wenn also die automatisierte Aufklärungstechnik das Risiko für objektiv Unbeteiligte erhöht, Ziel weiterer polizeilicher Aufklärungsmaßnahmen zu werden (vgl. dazu BVerfGE 115, 320 <351 ff.>; 120, 378 <403>; 125, 260 <320>). Insofern können mit einer weitergehenden Automatisierung von Polizeiarbeit jenseits des Potenzials, eine Diskriminierung zu verhindern auch spezifische Diskriminierungsrisiken einhergehen, die verfassungsrechtlich umso weniger hinzunehmen sind, je mehr sich die Wirkungen der automatisierten Datenanalyse oder -auswertung einer nach Art. 3 Abs. 3 GG unzulässigen Benachteiligung annähern könnten (vgl. zur Rasterfahndung BVerfGE 115, 320 <352 f.>; s. auch BVerfGE 154, 152 <259 Rn. 192>; näher Rademacher, AöR 142 <2017>, S. 366 <376 f.>; Wischmeyer, AöR 143 <2018>, S. 1 <26 ff.>; Martini, Blackbox Algorithmus, 2019, S. 88 f. m.w.N.). 77

(2) Das Eingriffsgewicht wird vor allem durch Art und Umfang der verarbeitbaren Daten bestimmt. Eine wesentliche Besonderheit des Eingriffspotenzials von Maßnahmen der elektronischen Datenverarbeitung liegt in der Menge der verarbeiteten Daten, die konventionell gar nicht bewältigt werden könnte (vgl. BVerfGE 156, 63 <118 f. Rn. 198> m.w.N.). Je größere Mengen personenbezogener Daten in die automatisierte Datenanalyse und -auswertung einbezogen werden können, je weniger der Gesetzgeber also die verwendbare Datenmenge begrenzt, umso schwerer wiegt der Eingriff. Eng mit der Regelung der Menge der verwendbaren Daten hängt auch die 78

Regelung der Art der verwendbaren Daten zusammen. Je weniger die verwendbaren Daten der Art nach eingeschränkt sind, umso größer ist die zur Verarbeitung gelangende Datenmenge und umso höher ist tendenziell das Eingriffsgewicht. Die Art der Daten ist aber auch für sich genommen für das Eingriffsgewicht von Bedeutung, weil die Verwendung unterschiedlicher Daten direkt oder mittelbar unterschiedliche Persönlichkeitsrelevanz entfalten kann. Die Art und der Umfang der einbezogenen Daten und deren Auswirkungen auf das Gewicht des Grundrechtseingriffs können durch verschiedene Vorkehrungen näher bestimmt und beschränkt sein.

(a) Das Gewicht des Eingriffs kann durch gesetzliche Regeln über die Herkunft der Daten reduziert sein, etwa durch eine Begrenzung auf Daten, die die Behörde selbst erhoben hat oder die eine andere Behörde desselben Landes, jedenfalls aber eine andere inländische Behörde erhoben hat, durch den Ausschluss von Daten, die aus sozialen Netzwerken erhoben wurden, eine Begrenzung auf schon ursprünglich von einer polizeilichen Behörde (des betroffenen Landes) erhobene Daten oder durch einen Ausschluss von Daten, die ursprünglich von nachrichtendienstlichen Behörden erhoben wurden. 79

(b) Die verwendbaren Daten können auch mit Blick auf die Umstände der Ersterhebung gesetzlich nach Art und Menge begrenzt sein. Insbesondere Regelungen zur Sicherung der Zweckbindung (Rn. 55 ff.) tragen zugleich zu einer Begrenzung des Datenumfangs bei. Wenn durch organisatorische oder technische Vorkehrungen gesichert wird, dass Daten nur ihrer rechtlichen Verwendbarkeit gemäß weiterverarbeitet werden und wenn die rechtliche Verwendbarkeit hinreichend eng gefasst ist, kann dies den Umfang der verarbeitbaren Daten erheblich reduzieren. Technisch-organisatorische Sicherungen, die die Einhaltung der Zweckbindung sicherstellen, können etwa in der technischen Trennung von Datenbeständen nach unterschiedlichen Verarbeitungszwecken oder in einer zweckabhängigen Verteilung von Zugriffsrechten auf Datenbestände bestehen (vgl. Bäuerle, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, Stand: 1. Oktober 2022, § 20 HSOG, Rn. 105). 80

Eingriffsmildernd wirkt auch der Ausschluss der Verarbeitung von Daten, die ursprünglich durch besonders schwere Grundrechtseingriffe erlangt wurden (so etwa § 6a Abs. 3 i.V.m. § 4 ATDG). Allerdings dürfen Daten, die aus einer Wohnraumüberwachung oder aus einer Online-Durchsuchung gewonnen wurden, in eine der vorbeugenden Bekämpfung von Straftaten dienende Datenanalyse oder -auswertung ohnehin nur unter sehr engen Voraussetzungen einbezogen werden; wegen des besonderen Eingriffsgewichts ließe sich dies nicht bei einer unterhalb der dringenden oder im Einzelfall hinreichend konkretisierten Gefahr liegenden Eingriffsschwelle rechtfertigen (vgl. BVerfGE 141, 220 <326 Rn. 283; 329 Rn. 291>). Auch Daten, die aus anderen schwerwiegenden Grundrechtseingriffen gewonnen wurden, dürfen in eine der vorbeugenden Bekämpfung von Straftaten dienende Datenanalyse oder -auswertung schon nach dem Grundsatz der Zweckbindung zweckändernd nur dann einbezogen werden, wenn sich hieraus im Einzelfall konkrete Ermittlungsansätze zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren ergeben (vgl. BVerfGE 81

141, 220 <329 Rn. 290>; s. auch oben Rn. 63).

Neben den Zweckbindungsregelungen kann eine herkunftsbezogene Eingrenzung der Daten auch dadurch erfolgen, dass nur Daten in die automatisierte Anwendung einbezogen werden, die bei der Wahrnehmung bestimmter polizeilicher Aufgaben angefallen sind (vgl. etwa § 2 Satz 1 1. Halbsatz ATDG – nur Daten aus der Terrorismusbekämpfung). 82

(c) Die Datenmenge lässt sich auch durch einen engeren Zuschnitt der mit der Datenanalyse oder -auswertung vorbeugend zu bekämpfenden Straftaten begrenzen, indem nur Daten verwendet werden, deren Einbeziehung für die Bekämpfung dieser näher eingegrenzten Straftaten erforderlich ist (vgl. etwa § 2 Satz 1 a.E. ATDG). 83

(d) Eingriffsmildernd wirkt zudem, wenn lediglich Daten Verwendung finden, die sich auf Personen beziehen, bezüglich derer die Polizei tatsächliche Anhaltspunkte besitzt, dass diese selbst in (hinreichend gewichtige) Straftaten verfangen sind oder dass sie Kontaktperson zu einer solchen Person sind (vgl. etwa § 2 und § 3 Abs. 2 ATDG). Hierdurch würde das Risiko reduziert, dass Informationen über Personen gewonnen werden, die selbst keinen zurechenbaren Anlass gegeben haben und dann anlassfrei operativen Folgemaßnahmen der Polizei ausgesetzt sein könnten. 84

(e) Die Datenmenge wird auch durch Regelungen über Aufbewahrungsfristen und Löschungspflichten bestimmt. Soweit mit der Einbeziehung von Verkehrsdaten, insbesondere den aus Funkzellenabfragen gewonnenen Daten (vgl. etwa § 100g Abs. 3 StPO), in den für die automatisierte Datenanalyse oder -auswertung bereitstehenden Datenpool eine breitere bevorratende Speicherung von Verkehrsdaten möglich ist, müssen jedenfalls die erfassbaren Datenmengen substantiell begrenzt und eine Höchstspeicherungsdauer geregelt sein (vgl. für die nachrichtendienstliche Ausland-Ausland-Fernmeldeaufklärung BVerfGE 154, 152 <259 Rn. 191>). 85

Als das Eingriffsgewicht mindernd ist hingegen einzustellen, wenn in die Datenanalyse oder -auswertung zwar eine große Zahl von Daten vieler überwiegend nichtbeteiligter Personen einbezogen wird, der Datenabgleich aber in Sekundenschnelle durchgeführt wird und die erfassten Daten im Nichttrefferfall keine weitere polizeiliche Tätigkeit veranlassen (vgl. BVerfGE 150, 244 <283 Rn. 97>). 86

(f) Darüber hinaus kann eine Regelung zugelassener Datenarten (vgl. etwa § 3 Abs. 1 ATDG) je nach der inhaltlichen Ausgestaltung begrenzende Wirkung entfalten. Das gilt auch für eine Regelung der einbeziehbaren Dateiformate, wie etwa von Bildern, Video- und Audioaufnahmen in die Datenanalyse oder -auswertung. Eingriffsmildernd kann etwa der Ausschluss biometrischer Daten wirken. 87

(g) Praktisch kann zur Reduktion der Menge verarbeitbarer Daten auch beitragen, wenn vorgegeben wird, dass Dateien nicht automatisiert einbezogen werden, sondern für jeden Analyse- oder Auswertungsvorgang händisch hinzugezogen werden müssen. Eingriffsverstärkend wirkt demgegenüber etwa eine Verknüpfung der Analyse- oder Auswertungseinrichtung mit dem Internet, weil dies die Verarbeitung be- 88

sonders großer Datenmengen praktisch fördert.

(h) Auch eine technisch und organisatorisch gesicherte Beschränkung des Zugriffs lediglich einer begrenzten Zahl von Mitarbeitenden und eine besondere Qualifizierung dieser Personen kann praktisch die Menge der durch Datenanalyse oder -auswertung verarbeitbaren personenbezogenen Daten begrenzen. Je weniger Personen Zugriff auf das Analyseinstrument haben und je zielgenauer der Zugriff erfolgt, umso weniger Analyse- oder Auswertungsvorgänge dürften tendenziell in Gang gesetzt werden und umso weniger Daten werden verarbeitet. 89

(3) Daneben beeinflusst die zugelassene Methode der Datenanalyse oder -auswertung die Eingriffsintensität. Besonderes Eingriffsgewicht kann der Einsatz komplexer Formen des Datenabgleichs haben. Wenn die Polizei aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen, daraus neue Zusammenhänge erschließen, aus mehrstufigen Analysen neue Verdachtsmomente erzeugen und hieran weitere Analyseschritte oder operative Maßnahmen anschließen kann, können die Nachteile auf Grund einer automatisierten Datenanalyse oder -auswertung für die Betroffenen erheblich sein und das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen (vgl. BVerfGE 156, 11 <39 f. Rn. 73> m.w.N.). Bei komplexen Formen des Datenabgleichs besteht zudem mit Blick auf individuellen Rechtsschutz und aufsichtliche Kontrolle und die dafür unerlässliche Möglichkeit, Fehler zu erkennen und zu korrigieren, die Schwierigkeit der Nachvollziehbarkeit der eingesetzten Algorithmen (vgl. BVerfGE 154, 152 <259 f. Rn. 192>). Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffsintensiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können. 90

(a) Das Eingriffsgewicht wird geringer, je mehr der Vorgang der automatisierten Datenanalyse oder -auswertung methodisch einem einfachen Datenabgleich angenähert ist. Beim einfachen Abgleich erfolgt die Suche nach einem vorhandenen Datenbestand etwa über eine Person, indem im jeweiligen System die eingegebenen Daten des Betroffenen an den gespeicherten Daten vorbeigeführt werden; als automatisches Datenverarbeitungsverfahren führt der Dateienabgleich insoweit regelmäßig Datenbestände zusammen, um Übereinstimmungen der Daten festzustellen oder Daten des einen Bestands in den anderen zu überführen (vgl. Bäuerle, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, 27. Edition, Stand: 1. Oktober 2022, § 25 HSOG, Rn. 9 f.). Der einfache Abgleich ist also ein suchender Vergleich von Daten zur Feststellung von Übereinstimmungen (vgl. auch Hamburgische Bürgerschaft AusschussDrucks 21/40, Anlage 1, S. 6). 91

Die Komplexität des suchenden Vergleichs kann sich allerdings durch eine höhere Zahl an Abgleichschritten und Verknüpfungen erhöhen. Ist die Zahl der vorprogrammierten Abgleichschritte, die sich ohne weiteren, im Einzelfall menschlich veranlass- 92

ten Anstoß vollziehen könnten, aber von vornherein begrenzt, reduziert dies die Verknüpfungsmöglichkeiten und trägt zur Senkung des Eingriffsgewichts bei.

(b) Das Eingriffsgewicht ist dagegen umso höher, je offener die Methode des Such- 93
vorgangs gestaltet ist und je weniger die automatisierte Datenanalyse oder -auswertung durch – auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste – polizeiliche Suchmuster gesteuert wird. Denn je offener ein automatisierter Suchvorgang zur vorbeugenden Bekämpfung von Straftaten im Vorfeld konkreter Gefahren ausgestaltet ist, je weniger Sachverhaltsbezug die Suche also hat, umso eher werden durch die Suche überhaupt erst Anhaltspunkte für eine Gefahr generiert. Das Eingriffsgewicht erhöht sich insbesondere, wenn die Datenanalyse oder -auswertung nicht auf einem Suchbegriff, jedenfalls nicht auf einem auf den bislang erkennbaren Sachverhalt bezogenen Suchbegriff gründet, sondern darauf zielt, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, die darüber hinaus (automatisiert) in weiteren Abgleichschritten mit bestimmten Datenbeständen verknüpft werden und so zu weiteren Informationen führen können, nach denen zu suchen die Polizei zuvor keinen Anlass hatte.

Der Grundrechtseingriff gewinnt auch an Gewicht, wenn Suchvorgänge nicht auf 94
näher umschreibbare Personen ausgerichtet sind und keine sachliche Verbindung zwischen dem gefährdeten Rechtsgut und den von der automatisierten Anwendung Betroffenen vorausgesetzt wird. Es fehlt dann jede tatsachengestützte Verbindung zu einer konkret verantwortlichen Person. Ein solcher Bezug wird dann überhaupt erst durch die Maßnahme hergestellt, und es steigt das Risiko, dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben (vgl. auch BVerfGE 115, 320 <361 f.>; BVerfG, Beschluss des Ersten Senats vom 9. Dezember 2022 - 1 BvR 1345/21 -, Rn. 189 – zur Rasterfahndung).

Die mit einer offenen Suche verbundenen Gefahren werden durch eine anspruchs- 95
voll ausgestaltete Eingriffsschwelle verringert (Rn. 104 ff.), können aber auch schon durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden, wenn der Suchvorgang eingrenzend so geregelt ist, dass er einen Bezug zu einem konkreteren Suchanlass voraussetzt. Je geringere Anforderungen der Gesetzgeber an den Anlass einer Datenanalyse oder -auswertung stellt, umso genauer und enger muss er die Methode der Suche regeln. Eine weder im Einzelfall durch einen konkreten Anlass getragene noch durch Vorgaben zur Verarbeitungsmethode inhaltlich eingeschränkte automatisierte Durchsuchung großer Bestände personenbezogener Daten auf bislang unbekannte Gesetzmäßigkeiten und gefahrenabwehrrechtlich bedeutende Zusammenhänge hin ist verfassungsrechtlich unzulässig. Erlaubt die gesetzlich zugelassene Methode eine Auswertung großer Datenmengen insbesondere auch auf statistische Zusammenhänge hin, ist zudem eine ausreichende Datenqualität sicherzustellen und es müssen Vorkehrungen dagegen getroffen sein, dass die Auswahl der einbezogenen Daten unangemessen verzerrende, diskriminierende Wirkungen entfalten kann (vgl. Rn. 77).

(c) Das Eingriffsgewicht hängt zudem davon ab, welche Art von Suchergebnissen durch eine automatisierte Datenanalyse oder -auswertung erzielt wird. 96

So ist das Eingriffsgewicht regelmäßig geringer, wenn die Datenanalyse oder -auswertung nicht auf personenbezogene Erkenntnisse, sondern etwa auf die Erkennung gefährlicher oder gefährdeter Orte zielt. 97

Besonders eingriffsintensiv ist hingegen, wenn Ergebnis der automatisierten Anwendung personenbezogene Erkenntnisse sind und dieses Ergebnis maschinelle Sachverhaltsbewertungen enthält, die also über die bloße Anzeige von Übereinstimmungen zwischen dem Suchkriterium und den durchsuchten Daten hinausgehen. Eingriffsintensivierend ist insbesondere, wenn im Sinne eines „predictive policing“ maschinell Gefährlichkeitsaussagen über Personen getroffen werden (vgl. dazu Rademacher, AöR 142 <2017>, S. 366 ff. m.w.N.). 98

(d) Das Gewicht des in der Erlangung neuen Wissens durch eine automatisierte Datenanalyse liegenden eigenen Eingriffs in die informationelle Selbstbestimmung kann sich aber dadurch verringern, dass die Verwendung dieser neuen Informationen an spezifische Voraussetzungen geknüpft wird. Denn für das Gewicht des Eingriffs in die informationelle Selbstbestimmung ist generell auch von Bedeutung, wie die gewonnenen personenbezogenen Informationen weiterverwendet werden und welche Folgen dies für die Betroffenen haben kann (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 157 m.w.N.; stRspr). 99

(e) Besonderes Eingriffsgewicht kann je nach Einsatzart die Verwendung lernfähiger Systeme, also Künstlicher Intelligenz (KI), haben. Deren Mehrwert, zugleich aber auch ihre spezifischen Gefahren liegen darin, dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden. Mittels einer automatisierten Anwendung könnten so über den Einsatz komplexer Algorithmen zum Ausweis von Beziehungen oder Zusammenhängen hinaus auch selbstständig weitere Aussagen im Sinne eines „predictive policing“ getroffen werden. So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein (vgl. EuGH, Urteil vom 21. Juni 2021, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, Rn. 195). Dann droht zugleich die staatliche Kontrolle über diese Anwendung verloren zu gehen. Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte (vgl. Wissenschaftlicher Dienst des Deutschen Bundestags, Datenbank-Analysen durch die Polizei. Grundrechte und Datenschutzrecht, 2. März 2020, WD3-3000-018/20, S. 8 100

m.w.N.). Eine spezifische Herausforderung besteht darüber hinaus darin, die Herausbildung und Verwendung diskriminierender Algorithmen zu verhindern. Daher dürften selbstlernende Systeme in der Polizeiarbeit nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern.

Aber auch die Auswertungsvorgänge deterministischer Systeme, deren Analysefunktion sich also nicht eigenständig verändern kann, sondern in der Software unveränderlich vorprogrammiert ist, können komplex und für die Anwendenden und Betroffenen schwer nachvollziehbar sein. Können eingriffsintensive Methoden der Datenauswertung, insbesondere komplexe Formen des Datenabgleichs zum Einsatz kommen, muss der Gesetzgeber für schützende Regelungen sorgen (vgl. BVerfGE 154, 152 <259 f. Rn. 192>). 101

(f) Wie schwer Eingriffe durch automatisierte Datenanalyse oder -auswertung wiegen, hängt insgesamt auch davon ab, wie fehleranfällig die eingesetzte Datenauswertungstechnologie ist und ob gegebenenfalls Vorkehrungen zur Entdeckung und Korrektur von Fehlern getroffen sind. 102

cc) Mit der vom Gesetzgeber durch Regelungen zu Art und Umfang der Daten und zur Begrenzung der Auswertungsmethode steuerbaren Eingriffsintensität korrespondieren die verfassungsrechtlichen Anforderungen an die Eingriffsvoraussetzungen. Ob eine Ermächtigung zur automatisierten Datenanalyse oder -auswertung verfassungsrechtlichen Anforderungen genügt, hängt mithin auch davon ab, ob der Gesetzgeber angesichts der konkreten Ausgestaltung der Befugnis ausreichende Eingriffsvoraussetzungen geregelt hat. Die dem Eingriffsgewicht entsprechenden Anforderungen des Gebots der Verhältnismäßigkeit im engeren Sinne richten sich sowohl an das mit der Maßnahme zu schützende Rechtsgut als auch an die Eingriffsschwelle, also den Anlass der Maßnahme (vgl. auch BVerfGE 141, 220 <269 Rn. 104, 270 f. Rn. 106 ff., 271 ff. Rn. 109 ff.>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 174; Beschluss des Ersten Senats vom 9. Dezember 2022 - 1 BvR 1345/21 -, Rn. 89; dazu unten Rn. 104 ff.). Wie ausgeführt (Rn. 75 ff.), stehen dem Gesetzgeber dabei vielfältige Möglichkeiten zur Verfügung, um das Gewicht des mit einer automatisierten Datenanalyse oder -auswertung verbundenen Eingriffs in die informationelle Selbstbestimmung so zu steuern, dass es in einem angemessenen Verhältnis zur jeweiligen Eingriffsschwelle und zum Gewicht der bezweckten Gefahrenprävention steht (vgl. auch BVerfGE 115, 320 <360>). Ermöglicht die automatisierte Anwendung einen eigenständig schweren Eingriff in die informationelle Selbstbestimmung der Betroffenen, ist dies nur unter engen Voraussetzungen zu rechtfertigen (1). Weniger gewichtige Eingriffe können schon aus geringerem Anlass zu rechtfertigen sein (2). Unter Umständen kann sogar die Einhaltung des Grundsatzes der Zweckbindung ausreichen (3). In jedem Fall ergeben sich aus dem Verhältnismäßigkeitsgrundsatz Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle (4). 103

(1) Ermöglicht die automatisierte Anwendung einen nach den genannten Kriterien schwerwiegenden Eingriff in die informationelle Selbstbestimmung der Betroffenen, ist dies nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten. 104

(a) Es sind dann hohe Anforderungen an das durch die automatisierte Datenanalyse oder -auswertung zu schützende Rechtsgut zu stellen. Heimliche Überwachungsmaßnahmen, die tief in das Privatleben hineinreichen, sind nur zum Schutz besonders gewichtiger Rechtsgüter zulässig (BVerfGE 141, 220 <270 Rn. 108>). Zu den besonders gewichtigen Rechtsgütern zählen vor allem Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes (vgl. BVerfGE 133, 277 <365 Rn. 203>; 141, 220 <270 f. Rn. 108, 328 ff. Rn. 288, 292>; 154, 152 <269 Rn. 221>; 156, 11 <55 Rn. 116>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 243). Vergleichbares Gewicht entfalten kann der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, sofern darunter einem engen Verständnis folgend etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen gefasst werden (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 244, unter Verweis auf BVerfGE 141, 220 <296 Rn. 183> sowie BVerfGE 133, 277 <365 Rn. 203>). Auch kann der Gesetzgeber darauf verzichten, das erforderliche Rechtsgut unmittelbar zu benennen und stattdessen an entsprechende Straftaten anknüpfen, deren Verhütung mit der Befugnis bezweckt ist (vgl. BVerfGE 154, 152 <269 Rn. 221>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 244). 105

(b) Auch der Eingriffsanlass muss dann streng begrenzt sein. Die verfassungsrechtlich erforderliche Eingriffsschwelle ist hier wie für die meisten heimlichen, tief in die Privatsphäre eingreifenden Überwachungsmaßnahmen der Gefahrenabwehrbehörden die hinreichend konkretisierte Gefahr (dazu im Einzelnen BVerfGE 141, 220 <272 f. Rn. 112>). Das ist die allgemeine Eingriffsschwelle für heimliche Überwachungsmaßnahmen der Gefahrenabwehrbehörden (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 248 m.w.N.). Eine hinreichend konkretisierte Gefahr setzt voraus, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen. Allgemeine Erfahrungssätze reichen insoweit allein nicht aus. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen. Eine hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so 106

viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfGE 141, 220 <272 Rn. 112>).

(2) Hingegen können weniger gewichtige Eingriffe beim Vorliegen einer konkretisierten Gefahr bereits dann zu rechtfertigen sein, wenn sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen, wie dies etwa bei der Verhütung von Straftaten von zumindest erheblicher Bedeutung der Fall ist. Umgekehrt kann dann eine Eingriffsschwelle genügen, die noch hinter einer konkretisierten Gefahr zurückbleibt, wenn die Maßnahme dem Schutz hochrangiger, überragend wichtiger oder auch besonders gewichtiger Rechtsgüter dient (vgl. BVerfGE 155, 119 <188 f. Rn. 150> m.w.N.). Während also bei eingriffsintensiven Maßnahmen eine konkretisierte Gefahr und der Schutz besonders gewichtiger Rechtsgüter zusammenkommen müssen, genügt bei weniger eingriffsintensiven Maßnahmen, wenn die gesetzliche Ermächtigungsnorm eine konkretisierte Gefahr oder den Schutz besonders gewichtiger Rechtsgüter voraussetzt (vgl. BVerfG, Beschluss des Ersten Senats vom 9. Dezember 2022 - 1 BvR 1345/21 -, Rn. 173). Dies kommt hier insbesondere dann in Betracht, wenn der Gesetzgeber das Eingriffsgewicht der Datenanalyse oder -auswertung durch eine strengere Regelung zu Art und Umfang der verwertbaren Daten und zur Verarbeitungsmethode verringert. 107

(3) Sind die einbeziehbaren Daten gesetzlich nach Art und Umfang in einer Weise reduziert und die möglichen Methoden der automatisierten Analyse oder Auswertung von vornherein so eingeschränkt, dass eine auf die Befugnis gestützte Maßnahme nicht zu tieferen Einsichten in die persönliche Lebensgestaltung der Betroffenen führt als sie die Behörde, wenngleich aufwendiger und langsamer, auch ohne automatisierte Anwendung realistisch erlangen könnte, oder zielt die Befugnis von vornherein nur darauf, gefährliche oder gefährdete Orte zu identifizieren, ohne dabei personenbezogene Informationen zu generieren, kann sogar die Einhaltung des Grundsatzes der Zweckbindung ausreichen, um die weitere Verarbeitung der Daten in einer automatisierten Anwendung zu rechtfertigen (Rn. 55). Eine gänzlich anlasslose automatisierte Auswertung personenbezogener Daten durch Polizeibehörden zur vorbeugenden Bekämpfung von Straftaten wäre zwar verfassungsrechtlich unzulässig; die Einhaltung des verfassungsrechtlichen Grundsatzes der Zweckbindung sichert dann jedoch, dass es einen Eingriffsanlass gibt. 108

(4) Der Verhältnismäßigkeitsgrundsatz stellt hier in jedem Fall auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle (vgl. BVerfGE 141, 220 <282 Rn. 134> m.w.N.; stRspr). Insbesondere einer sachgerechten Ausgestaltung der Kontrolle kommt große Bedeutung zu. Diese kann angesichts der möglicherweise hohen Zahl von Maßnahmen etwa nach einem abgestuften Kontrollkonzept zwischen unabhängigen und behördlichen Datenschutzbeauftragten aufgeteilt und auch als stichprobenartiges Vorgehen geregelt werden. Für eine effektive Kontrolle unerlässlich ist dabei, dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden. Wird Software einge- 109

setzt, die komplexere Formen des automatisierten Abgleichs von Daten erlaubt, sind auch Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit erforderlich, was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann. Welche Anforderungen an den flankierenden Schutz im Einzelnen zu stellen sind, ist nicht Gegenstand dieses Verfahrens.

dd) Die Schwelle einer wenigstens konkretisierten Gefahr für besonders gewichtige Rechtsgüter ist nur dann verfassungsrechtlich verzichtbar, wenn die zugelassenen Analyse- und Auswertungsmöglichkeiten normenklar und hinreichend bestimmt in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahmen erheblich gesenkt ist. Grundsätzlich kann der Gesetzgeber diese Regelungsaufgabe zwischen sich und der Verwaltung aufteilen (1). Er muss aber sicherstellen, dass unter Wahrung des Gesetzesvorbehalts insgesamt ausreichende Regelungen insbesondere zur Begrenzung von Art und Umfang der Daten (2) und zur Beschränkung der Datenverarbeitungsmethoden (3) getroffen werden. 110

Ob der Gesetzgeber ergänzende Regelungen zur Begrenzung von Art und Umfang der Daten und zur Beschränkung der Verarbeitungsmethoden auch dann treffen muss, wenn er die Datenanalyse und -auswertungsbefugnis an die strenge Voraussetzung einer wenigstens konkretisierten Gefahr für besonders gewichtige Rechtsgüter bindet, muss hier nicht beantwortet werden. Gegenstand ist hier auch nicht, ob die verfassungsrechtlichen Anforderungen der Zweckbindung für die Datenanalyse oder -auswertung hinreichend gesetzlich geregelt sind und ob hinreichende Regelungen zu Transparenz, individuellem Rechtsschutz und aufsichtlicher Kontrolle bestehen (Rn. 48). Damit stellt sich hier insoweit auch die Frage der Vereinbarkeit mit dem Gesetzesvorbehalt nicht. 111

(1) Will der Gesetzgeber der Polizei eine Befugnis zur automatisierten Datenanalyse oder -auswertung – wie hier – bereits für die vorbeugende Bekämpfung von Straftaten, also im Vorfeld einer konkretisierten Gefahr einräumen, muss er zur Wahrung der Verhältnismäßigkeit die Eingriffsintensität der Maßnahme reduzieren. Bei den hierfür bestehenden Möglichkeiten zur Begrenzung insbesondere von Art und Umfang der Daten und der Verarbeitungsmethoden sind die Anforderungen des Gesetzesvorbehalts zu beachten. Der Gesetzgeber muss die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben. Wegen der besonderen Technizität und der raschen Fortentwicklungsbedürftigkeit der hier zur Milderung des Eingriffs benötigten Regelungen kann er, soweit eine tiefergehende gesetzliche Normierung nicht praktikabel erscheint, die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigen. Er muss aber sicherstellen, dass im Zusammenwirken der gesetzlichen Vorgaben mit den Regelungsermächtigungen und -verpflichtungen der Verwaltung Art und Umfang der Daten und die Verarbeitungsmethoden insgesamt inhaltlich ausreichend, normenklar und transparent begrenzt sind. 112

Zur Regelung von Aspekten, die nicht unmittelbar vom Gesetzgeber selbst zu normieren sind, kommt zunächst eine Verordnungsermächtigung in Betracht. Darüber hinaus kann der Gesetzgeber hier die Verwaltung verpflichten, die im Gesetz oder in Rechtsverordnungen geregelten Vorgaben in abstrakt-genereller Form weiter zu konkretisieren. In jedem Fall bedarf die Konkretisierung durch Verwaltungsvorschriften aber einer gesetzlichen Grundlage. Darin hat der Gesetzgeber sicherzustellen, dass die für die Anwendung der Bestimmungen im Einzelfall maßgebliche Konkretisierung und Standardisierung seitens der Behörden nachvollziehbar dokumentiert und veröffentlicht wird (vgl. auch BVerfGE 133, 277 <357 Rn. 183>). Sind die Vorgaben zu Art und Umfang der in die automatisierte Datenanalyse oder -auswertung einbeziehbaren Daten und der zulässigen Verarbeitungsmethoden aus dem Gesetz selbst nur begrenzt erkennbar, bedürfen sie nachvollziehbarer Konkretisierung und Standardisierung durch die Verwaltung. Es ist dann auch deshalb ein Ausgleich durch besondere Transparenzanforderungen an die Verwaltung geboten, weil die Durchführung einer automatisierten Datenanalyse oder -auswertung in der Regel von den Betroffenen nicht wahrgenommen wird und sich die Konkretisierung der gesetzlichen Vorgaben damit kaum im Wechselspiel von Verwaltungsakt und gerichtlicher Kontrolle vollzieht. Mangels verwaltungsgerichtlicher Kontrolle fällt somit ein zentraler Mechanismus notwendiger Begrenzung konkretisierungsbedürftiger Befugnisnormen weitgehend aus. Um diese Besonderheit auszugleichen, hat der Gesetzgeber zu gewährleisten, dass die Verwaltung die für die Durchführung einer automatisierten Datenanalyse oder -auswertung im Einzelfall maßgeblichen Vorgaben und Kriterien in abstrakt-genereller Form festlegt und verlässlich dokumentiert wie auch in einer vom Gesetzgeber näher zu bestimmenden Weise veröffentlicht. Eine solche Festlegung, Dokumentation und Offenlegung dient zum einen der Einhegung der der Verwaltung eingeräumten Befugnisse. Zum anderen sichert sie ein hinreichendes Kontrollniveau. Denn die Dokumentation und Offenlegung der von der Verwaltung festgelegten Kriterien versetzt insbesondere die Datenschutzbeauftragten in die Lage, die Anwendung der Befugnis durch die Exekutive zu kontrollieren (vgl. BVerfGE 133, 277 <357 f. Rn. 184> m.w.N.). 113

Der Gesetzgeber muss die von ihm selbst zu normierenden Maßgaben auch hinreichend bestimmt und normenklar regeln (vgl. dazu BVerfGE 156, 11 <45 f. Rn. 86 f.>). Soweit sich Maßgaben zur Eingrenzung zulässiger Datenverarbeitung bereits aus Vorschriften des allgemeinen oder des polizeilichen Datenschutzrechts ergeben, muss deren Anwendbarkeit auf die Datenanalyse oder -auswertungsbefugnis sowohl für die Behörde als auch für Bürgerinnen und Bürger hinreichend deutlich erkennbar sein, und es muss auch hinreichend klar sein, was daraus für die praktische Ausgestaltung gerade der Datenanalyse oder -auswertungsbefugnis folgt. 114

(2) Will der Gesetzgeber die Eingriffsintensität der automatisierten Datenanalyse oder -auswertung verringern, um dieses Instrument auch im Vorfeld einer konkretisierten Gefahr einsetzen zu können, muss er grundlegende Vorgaben zu Art und Umfang der in der automatisierten Datenanalyse oder -auswertung verwendbaren 115

Daten selbst regeln.

Im Gesetz selbst ist insbesondere zu regeln, welche Datenbestände einbezogen werden dürfen und inwiefern dies automatisiert erfolgen darf. Wenn der Gesetzgeber die verwendbaren Datenbestände nicht selbst abschließend aufzählt, muss er sicherstellen, dass dies untergesetzlich abstrakt-generell geregelt und veröffentlicht wird. Wie weit der Kreis (automatisiert) einbeziehbarer Datenbestände in der Sache gefasst werden kann, ist verfassungsrechtlich nicht starr vorgegeben. Jedoch ist die Eingriffsintensität umso höher, je größer und zahlreicher die verwendbaren Datenbestände sind (Rn. 78 ff.); entsprechend höher müssen dann die Anforderungen an den Eingriffsanlass und das zu schützende Rechtsgut ausfallen. 116

Sofern die für die automatisierte Datenanalyse oder -auswertung verwendbaren Datenbestände nicht von vornherein inhaltlich und mengenmäßig sehr eng begrenzt sind, muss der Gesetzgeber zur Begrenzung der automatisierten Anwendung zudem sicherstellen, dass nur einzelne, entsprechend qualifizierte Mitarbeiterinnen und Mitarbeiter der Polizei Zugriff auf die Einrichtung haben und davon nur in dem durch den gesetzlich zu regelnden Eingriffsanlass erforderlichen Zusammenhang Gebrauch machen können. Die Begrenzung der Zugriffsmöglichkeiten ist über die rechtliche Begrenzung hinaus durch organisatorische und technische Vorkehrungen sicherzustellen. Technische Einzelheiten können in zu veröffentlichenden Verwaltungsvorschriften geregelt werden. 117

Schon wegen des verfassungsrechtlichen Grundsatzes der Zweckbindung von Daten (Rn. 55 ff.) ist dagegen durch das Gesetz selbst zu regeln, dass Daten, die aus Wohnraumüberwachung oder Online-Durchsuchung gewonnen wurden, in eine der vorbeugenden Bekämpfung von Straftaten dienende Datenanalyse oder -auswertung nicht einbezogen werden dürfen (Rn. 59, 64). Auch soweit Daten aus anderen schwerwiegenden Grundrechtseingriffen gewonnen wurden, ist eine weitere Verwendung inhaltlich auf Konstellationen zu begrenzen, in denen sie Informationen enthalten, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter ergeben (Rn. 63). Der Gesetzgeber muss auch dies selbst regeln. Für beide Konstellationen muss er zudem regeln, dass die Einschränkung durch entsprechende technische und organisatorische Vorkehrungen wirksam gesichert wird, die den Besonderheiten einer automatisierten Datenanalyse oder -auswertung, insbesondere bei automatisierter Einbindung von Datenbeständen, Rechnung tragen. Insbesondere müssen Informationen aus eingriffsintensiver Datenerhebung vorab gekennzeichnet oder abgetrennt werden, um gegebenenfalls den Zugriff zu verhindern und dürfen nicht, wie der Prozessbevollmächtigte der Beschwerdeführenden im Verfahren 1 BvR 1547/19 befürchtet, erst nachträglich identifiziert werden (vgl. auch unten Rn. 144). Der Gesetzgeber kann dabei die konkrete Ausgestaltung entsprechender Schutzmaßgaben der Verwaltung überlassen, die diese aber normenklar abstrakt-generell regeln und veröffentlichen muss. Solange nicht auch praktisch sichergestellt ist, dass Daten, die aus besonders schwerwiegenden Grundrechtseingriffen gewonnen wur- 118

den, nur unter den genannten Voraussetzungen in die automatisierte Datenanalyse oder -auswertung einbezogen werden können, darf die Befugnis nicht zur vorbeugenden Bekämpfung von Straftaten eingesetzt werden.

Es bestehen weitere Möglichkeiten, das Eingriffsgewicht mit Blick auf Art und Umfang der in der automatisierten Datenanalyse oder -auswertung verwendbaren Daten zu mindern (Rn. 78 ff.). Auch insoweit gilt aber der Gesetzesvorbehalt. Zu einer Absenkung der verfassungsrechtlichen Anforderungen an die gesetzliche Eingriffsschwelle oder das zu schützende Rechtsgut führen weitere Einschränkungen also nur, wenn die begrenzenden Maßgaben im Wesentlichen im Gesetz selbst geregelt oder durch dieses vorgegeben und durch die Verwaltung klar abstrakt-generell geregelt, dokumentiert und veröffentlicht sind. 119

(3) Wenn der Gesetzgeber die Eingriffsintensität der automatisierten Datenanalyse oder -auswertung reduzieren will, um sie auch im Vorfeld einer konkretisierten Gefahr einsetzen zu können, muss er zudem einschränkende Vorgaben zur Methode der automatisierten Datenanalyse oder -auswertung machen und in ihren grundlegenden Zügen im Gesetz selbst regeln. 120

Der Einsatz selbstlernender Systeme muss dafür im Gesetz ausdrücklich ausgeschlossen sein. Darüber hinaus muss der Gesetzgeber selbst grundlegende Maßgaben zur Begrenzung des Automatisierungsgrades treffen. Es reicht nicht aus, dass die Polizeibehörden die Datenanalyse oder -auswertung faktisch so gestalten, dass sie nicht über einen einfachen Datenabgleich in automatisierter Form hinausgeht, insbesondere nicht automatisiert wiederholte Abgleichschritte zur Verknüpfung der Abgleichergebnisse mit weiteren Datenbeständen erfolgen. Eine Beschränkung der Abgleichmöglichkeiten müsste vielmehr im Gesetz selbst angelegt sein. Der Gesetzgeber müsste auch wenigstens im Ansatz selbst regeln, wenn er das Eingriffsgewicht dadurch vermindern will, dass der Auswertung zur Vermeidung völlig offener Suchvorgänge einzelne Suchbegriffe zugrunde gelegt werden, in denen sich polizeiliche Suchmuster abbilden (dazu Rn. 93 ff.). Er müsste auch selbst wenigstens grundlegende Maßgaben treffen, wenn er das Eingriffsgewicht durch eine Begrenzung möglicher Analyseergebnisse reduzieren will (dazu Rn. 96 ff.). Sollen etwa maschinelle Sachverhaltsbewertungen ausgeschlossen werden, die über die Anzeige von Übereinstimmungen zwischen Suchkriterium und durchsuchten Datenbeständen hinaus gehen, sollen insbesondere maschinelle Gefährlichkeitsaussagen über Personen im Sinne eines „predictive policing“ ausgeschlossen oder die Datenanalyse oder -auswertung von vornherein nur auf die Erkennung gefährlicher oder gefährdeter Orte gerichtet werden, ist das Eingriffsgewicht nur dann verringert, wenn der Gesetzgeber dies selbst vorgibt. Die nähere Strukturierung des Auswertungsvorgangs könnte allerdings der Verwaltung aufgegeben werden (vgl. auch BVerfGE 154, 152 <259 Rn. 192>), die auch dies abstrakt-generell regeln und ihre Regelung veröffentlichen müsste. 121

Im Übrigen bestehen weitere Möglichkeiten, das Eingriffsgewicht der automatisier- 122

ten Datenanalyse oder -auswertung mit Blick auf die Verarbeitungsmethode zu mindern (oben Rn. 90 ff.), was aber nur dann zu einer Absenkung der verfassungsrechtlichen Anforderungen an die gesetzliche Eingriffsschwelle oder das zu schützende Rechtsgut führen kann, wenn die begrenzenden Maßgaben dem Gesetzesvorbehalt genügen und weitere Maßgaben durch die Verwaltung abstrakt-generell geregelt, dokumentiert und veröffentlicht sind.

c) Nach den dargelegten generellen Maßstäben ist das spezifische Eingriffsgewicht der daten- und methodenoffen formulierten Befugnis zur Datenanalyse oder -auswertung nach § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG potenziell sehr hoch (aa), so dass diese Regelungen von Verfassungs wegen strengen Eingriffsvoraussetzungen genügen müssen (bb). 123

aa) Das Eingriffsgewicht der angegriffenen Befugnis zur Datenanalyse oder -auswertung ist hier nach Datenart und -umfang (1) und Verarbeitungsmethode (2) potenziell sehr hoch. 124

(1) Die beiden Vorschriften begrenzen die Art und die Menge der bei einer Datenanalyse oder -auswertung einsetzbaren Daten kaum. Sie regeln nicht, welche Arten von Daten und welche Datenbestände für eine automatisierte Datenanalyse oder -auswertung genutzt werden dürfen. 125

(a) Die Vorschriften unterscheiden insbesondere nicht nach Daten von Personen, die einen Anlass für die Annahme geben, sie könnten eine Straftat begehen oder in besonderer Verbindung zu solchen Personen stehen (vgl. § 2 ATDG), und anderen Personen, obwohl insbesondere aus den Datenbeständen der Vorgangsbearbeitung (unten Rn. 133 ff.) und aus Funkzellenabfragen (unten Rn. 142) sehr viele Daten zu Personen in die Datenanalyse oder -auswertung eingehen könnten, die keinen Anlass für Maßnahmen zu einer vorbeugenden Bekämpfung schwerer Straftaten geben. Auch Datenbestände aus der Strafverfolgung können solche Daten enthalten, etwa die von Opfern oder Zeugen. Selbst die Einbeziehung von Personen, die einmal strafrechtlich oder polizeilich verantwortlich waren und deren Daten nach § 20 Abs. 6 und 7 HSOG und § 36 Abs. 2 und 3 HmbPolDVG weiterverarbeitet werden können, sind dann häufig Nichtverantwortliche, denn die Normen fordern für die Einbeziehung solcher Daten keine Negativprognose (vgl. für § 20 Abs. 6 und 7 HSOG Bäuerle, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, 27. Edition, Stand: 1. Oktober 2022, § 20 HSOG, Rn. 117). Insgesamt lassen die Regelungen eine breite Einbeziehung von Daten Unbeteiligter zu (ebd., Rn. 123 f.), die deshalb weiteren polizeilichen Ermittlungsmaßnahmen unterzogen werden könnten, obwohl sie hierfür keinen zurechenbaren Anlass gegeben haben. 126

(b) Die Normen treffen keine Regelung darüber, welche Datenbestände einbezogen werden dürfen. § 49 HmbPolDVG begrenzt die Befugnis, anders als § 25a HSOG, zwar auf in polizeilichen Dateisystemen gespeicherte Daten. Das setzt jedoch nicht voraus, dass es sich um originär von der Polizei erhobene Daten handelt und grenzt auch nicht weiter ein, woher die aktuell in polizeilichen Dateisystemen gespeicherten 127

Daten stammen. Ausgeschlossen sind weder Daten aus anderen Bundesländern, aus dem Zuständigkeitsbereich des Bundes oder aus anderen Staaten. Noch ist ausgeschlossen, dass die Daten von anderen, nicht polizeilichen Behörden oder auch von nicht-öffentlichen Stellen erlangt wurden. Auch die Weiterverwendung von Daten, die seitens nachrichtendienstlicher Behörden erhoben und zur Abwehr einer wenigstens konkretisierten Gefahr (vgl. BVerfGE 156, 11 <55 Rn. 118>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 245; Beschluss des Ersten Senats vom 28. September 2022 - 1 BvR 2354/13 -, Rn. 132 ff. – Bundesverfassungsschutzgesetz – Übermittlungsbefugnisse) übermittelt wurden, schließen die Regelungen nicht ausdrücklich aus.

Die Frage einer automatisierten Einbindung von Datenbeständen in die Datenanalyse oder -auswertung ist ebenfalls nicht speziell geregelt. 128

Auch die nur in § 49 HmbPolDVG, nicht aber in § 25a HSOG verwendete Formulierung des „Dateisystems“ schränkt die verarbeitbaren Datenbestände nicht näher ein. Ein Dateisystem ist nach § 2 Abs. 13 HmbPolDVG jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. Typen und Zahl solcher polizeilichen Systeme oder deren Inhalt sind gesetzlich nicht vorgegeben. Der Begriff des „Dateisystems“ erfasst auch mehr als die systematisch betriebenen automatisierten Datenbanken. Ohnehin besteht die Möglichkeit, Dateisysteme – gegebenenfalls kurzfristig – neu zu schaffen. 129

(c) Allerdings könnte sich aus andernorts allgemein geregelten Weiternutzungsvorschriften ergeben, dass bestimmte Daten und Datenbestände nicht in die Datenanalyse oder -auswertung einbezogen werden dürfen. Um das Eingriffsgewicht von Maßnahmen nach §§ 25a HSOG, 49 HmbPolDVG verfassungsrechtlich maßgeblich senken zu können, müsste deren Geltung und praktische Anwendung für die automatisierte Datenanalyse oder -auswertung jedoch genauer geregelt werden. In den angegriffenen Vorschriften fehlt hierzu jede Maßgabe. Insbesondere fehlt eine Normierung entsprechender organisatorisch-technischer Vorkehrungen. 130

(aa) Grundsätzlich könnten allgemeine Regelungen über die weitere Nutzung von bereits erhobenen und gespeicherten Daten die Art und Menge der in eine Datenanalyse oder -auswertung einbeziehbaren Daten beschränken und damit das Eingriffsgewicht mindern. Für die Polizei in Hessen und in Hamburg ergeben sich Grenzen der Weiterverarbeitung insbesondere aus dem allgemeinen Grundsatz der Zweckbindung in § 20 HSOG und in § 34 HmbPolDVG. In diesem Verfahren hat sich allerdings gezeigt, dass die Bedeutung der allgemeinen Zweckbindungsregelungen in § 20 HSOG und in § 34 HmbPolDVG für die automatisierte Datenanalyse oder -auswertung teilweise ungewiss ist, diese Regelungen aber jedenfalls nicht in der erforderlichen Bestimmtheit und Normenklarheit zur Begrenzung des Eingriffsgewichts beitragen und eine begrenzende Wirkung auch aus praktischen Gründen nicht ohne 131

Weiteres entfalten können.

(α) So könnte, wie der Prozessbevollmächtigte der Freien und Hansestadt Hamburg in der mündlichen Verhandlung dargelegt hat, § 49 HmbPolDVG als Spezialregelung verstanden werden, die von den Zweckbindungsregelungen von vornherein befreit. Wegen der praktischen Schwierigkeiten, die Zweckbindung einzelner Daten bei dem gerade auf die Zusammenführung zu einem Datenpool und auf Automatisierung angelegten Instrument zu realisieren, ist dies fachrechtlich keine fernliegende Interpretation. 132

(β) Im hessischen Recht besteht Ungewissheit, ob § 20 Abs. 9 Satz 3 HSOG so zu verstehen ist, dass die allgemeinen Zweckbindungsregelungen in § 20 Abs. 1 und 2 HSOG für die Einbeziehung der großen Menge von Daten aus der Vorgangsverwaltung in die automatisierte Datenanalyse nach § 25a HSOG nicht gelten, beziehungsweise, ob § 20 Abs. 1 und 2 HSOG, wenn sie denn Anwendung finden, zu einer nennenswerten Beschränkung der Datenmengen führen. 133

Die Einbeziehung von Daten der Vorgangsbearbeitung trägt erheblich zum Volumen der Datenanalyse bei. Ein „Vorgang“ umfasst sämtliche Unterlagen, die im Zusammenhang einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder einen sonstigen Gegenstand polizeilichen Handelns geführt werden (vgl. Müller/Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt G, Rn. 832 m.w.N.). In den Vorgangsbearbeitungssystemen erfasst die Polizei Daten, die sie für ihre konkrete polizeiliche Aufgabe und Sachbearbeitung im Einzelfall benötigt. Aufgenommen werden insbesondere Anzeigen, Ermittlungsberichte und Vermerke – auch zu Verkehrsunfällen. Die Systeme enthalten auch Daten zu Personen, die Anzeige erstatten oder Hinweise geben, zu Zeugen, Unfallbeteiligten und anderen Personen, die nicht Verdächtige oder Beschuldigte im Sinne des Strafprozessrechts oder Verantwortliche im Sinne des Polizeirechts sind (vgl. Arzt, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt G, Rn. 1184 m.w.N.). In Hessen sind diese Daten automatisiert in die Analyseplattform eingebunden (vgl. auch Hamburgische Bürgerschaft AusschussDrucks 21/39, S. 20). 134

Ob für diese Daten der Vorgangsbearbeitung bei Einbeziehung in die automatisierte Datenanalyse die Einschränkungen des § 20 Abs. 1 und 2 HSOG gelten, ist demnach für den Umfang der Datenverarbeitung sehr bedeutend. Das ist aber weder klar geregelt noch praktisch eindeutig geklärt. Von einer Nichtgeltung waren der Hessische Beauftragte für Datenschutz und Informationsfreiheit und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in ihren schriftlichen Stellungnahmen ausgegangen. Der Wortlaut von § 20 Abs. 9 HSOG ließe diese Interpretation ohne Weiteres zu, zumal es Wille des Gesetzgebers war, mittels der automatisierten Analyse die Trennung der Datenbestände in der bisherigen Form zu überwinden (vgl. HessLTDrucks 19/6502, S. 40 f.). In der mündlichen Verhandlung haben hingegen das Ministerium wie auch der Hessische Beauftragte für Datenschutz und Informationsfreiheit vertreten, die allgemeine Zweckbindung gelte doch. § 20 Abs. 9 HSOG 135

regelt diese Frage nicht deutlich.

Davon abgesehen spricht das praktische Verständnis der Bedeutung von § 20 Abs. 2 Satz 1 Nr. 2 HSOG bei der Anwendung von § 25a HSOG dagegen, dass die Menge der verarbeitbaren Daten hierdurch nennenswert eingegrenzt werden könnte. In der mündlichen Verhandlung antwortete das Hessische Ministerium des Innern und für Sport auf die Frage, wie sich für jedes einzelne im Vorgangsbearbeitungssystem gespeicherte Datum sicherstellen lasse, dass sich daraus der in § 20 Abs. 2 Satz 1 Nr. 2 HSOG vorausgesetzte konkrete Ermittlungsansatz ergebe, aus kriminologischer Sicht könne man niemals ausschließen, dass Daten für den jeweiligen Straftatbestand, dessen Begehung mittels Datenanalyse vorbeugend bekämpft werden soll, von Bedeutung seien. Auf die Frage zur quantitativen Bedeutung der Daten der Vorgangsbearbeitung für die Datenanalyse wurde bekundet, diese Daten seien sehr wichtig; polizeilich kenne man keine Unbeteiligten, denn alle Personen, zu denen im Vorgangssystem etwas dokumentiert sei, seien hierdurch Beteiligte. Danach ist nicht ersichtlich, dass § 20 Abs. 2 Satz 1 Nr. 2 HSOG, selbst wenn er auf die Datenanalyse angewendet wird, den Umfang der aus dem Vorgangsbearbeitungssystem herangezogenen Daten in der Anwendungspraxis auf eine kleine Menge beschränkt (s. aber zu weiteren Eingrenzungen der hessischen Anwendungspraxis über das Tatbestandsmerkmal „Einzelfall“ unten Rn. 159 ff.). 136

Insgesamt ist der Datenumfang durch die allgemeinen Regelungen zur Zweckbindung jedenfalls nicht so klar eingegrenzt, dass hierdurch das Eingriffsgewicht der Datenanalyse oder -auswertung verfassungsrechtlich erheblich eingeschränkt würde. 137

(?) Bei der automatisierten Analyse oder Auswertung großer Datenbestände, die zudem teils automatisiert einbezogen werden, können Regelungen über die Zweckbindung ihre begrenzende Wirkung auch aus praktischen Gründen nicht ohne Weiteres entfalten, weil die Menge der Daten und deren teils automatisierte Einbindung eine Zweckidentifizierung und -prüfung für jedes einzelne Datum erschweren. 138

Es bestehen zwar Kennzeichnungsvorschriften (vgl. § 20a HSOG, § 65 HmbPolDVG). Von diesen wird jedoch umfänglich befreit (vgl. § 20a Abs. 4 HSOG, § 78 Abs. 1 HmbPolDVG). Praktisch findet hier nach übereinstimmenden Aussagen in der mündlichen Verhandlung derzeit keine Kennzeichnung statt. Ohnehin sorgte aber die Kennzeichnung allein noch nicht dafür, dass die durch die Zweckbindungsregelungen für die einzelnen Daten geltenden Grenzen eingehalten werden. Besonders schwierig erscheint dies bei einer automatisierten Einbindung von Dateien, zumal wenn es sich um große Datenbestände handelt. Eine begrenzende Wirkung gesetzlicher Zweckbindungsregelungen wird sich hier nur mittels organisatorischer und technischer Vorkehrungen realisieren lassen, die näher geregelt werden müssten, um das Eingriffsgewicht in verfassungsrechtlich anzuerkennender Weise reduzieren zu können. 139

Die allgemeinen Datenschutzregeln in § 20 Abs. 4 HSOG und § 66 HDSIG und in § 56 HmbPolDVG verpflichten zwar zu organisatorischen und technischen Vorkehrun- 140

gen, die die Einhaltung der Zweckbindung sicherstellen. Hierdurch wird der Zugriff auf Daten für eine automatisierte Datenanalyse oder -auswertung aber nicht hinreichend normenklar und bestimmt eingeschränkt. Dies müsste – jedenfalls mit Blick auf die Befugnis aus § 25a HSOG und § 49 HmbPolDVG – näher geregelt werden. Technisch-organisatorische Sicherungen, die die Einhaltung der Zweckbindung sicherstellen, können etwa in der technischen Trennung von Datenbeständen nach unterschiedlichen Verarbeitungszwecken oder einer zweckabhängigen Verteilung von Zugriffsrechten auf Datenbestände bestehen (vgl. Bäuerle, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, 27. Edition, Stand: 1. Oktober 2022, § 20 HSOG, Rn. 105). Die hessische Landesregierung hat mehrfach dargelegt, dass nach einem speziellen Rollen- und Rechtekonzept in unterschiedlichem Ausmaß Zugriff auf die Analyseplattform gestattet werde (vgl. auch Auskunft des Hessischen Innenministers, HessLTDrucks 20/661, S. 2). Ein solches Konzept kann im Grundsatz zu einer technisch-organisatorischen Sicherung der Zweckbindung geeignet sein, ist aber bislang nicht normiert. Der Gesetzgeber hat hierzu keine Vorgaben gemacht. Zwar heißt es in den Begründungen der Gesetzentwürfe zu § 25a HSOG und zu § 49 HmbPolDVG, welche Datenbestände für die Datenanalyse erforderlich sind, sei im Hinblick auf den jeweiligen Analysezweck zu prüfen und gegebenenfalls über Zugriffsberechtigungen zu definieren (vgl. HessLTDrucks 19/6502, S. 41; Hamburgische Bürgerschaft Drucks 21/17906, S. 70). Die angegriffenen Vorschriften selbst regeln dies jedoch nicht und ermächtigen und verpflichten auch die Verwaltung nicht zur Erstellung eines solchen Konzepts. Die Verwaltung hat in Hessen zwar ihr spezielles Rollen- und Rechtekonzept entwickelt und geht nach diesem vor, hat dies bislang jedoch nicht als abstrakt-generelle Regelung in einer öffentlich zugänglichen Weise dokumentiert.

(bb) Grundsätzlich könnten auch speziellere Regeln über die Weiterverarbeitung von Daten, die mittels besonders schwerer Grundrechtseingriffe erhoben worden sind, die Art und die Menge der in eine Datenanalyse oder -auswertung einbeziehbaren Daten beschränken. Für Daten aus der Strafverfolgung gilt insoweit zwar insbesondere § 479 Abs. 2 Satz 2 StPO. Ähnliche Vorgaben finden sich in § 34 Abs. 4 Satz 1 und § 36 Abs. 2 Satz 2 HmbPolDVG. § 20 Abs. 1 Satz 3 und Abs. 3 HSOG enthält Anforderungen an die Weiterverarbeitung von personenbezogenen Daten aus Wohnraumüberwachung und Online-Durchsuchung. Deren Anwendbarkeit auf die automatisierte Datenanalyse oder -auswertung ist aber nicht hinreichend geregelt und deren Wirkung ohnehin nicht durch Maßgaben zur technischen und organisatorischen Umsetzung praktisch hinreichend gesichert, um das Eingriffsgewicht der Datenanalyse oder -auswertung hierdurch erheblich zu mindern. 141

(α) Das gilt insbesondere, wenn in die automatisierte Datenanalyse oder -auswertung Verkehrsdaten aus Funkzellenabfragen einbezogen werden, aus denen sich sehr umfangreiche Datenbestände ergeben können. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat in der mündlichen Verhandlung erklärt, bei der Funkzellenabfrage enthalte eine Lieferung ungefähr 100.000 Daten. Der Hes- 142

sische Beauftragte für Datenschutz und Informationsfreiheit hat ausgeführt, es stünden Daten aus Funkzellenabfragen in Hessen aus den letzten zwei Jahren zur Verfügung. Allerdings ist deren weitere Verwendung zur Gefahrenabwehr, wenn sie nach § 100g Abs. 3 StPO erhoben wurden, durch § 479 Abs. 2 Satz 2 StPO eingeschränkt. Inwiefern eine entsprechende Einschränkung auch gelten würde, wenn Funkzellendaten nicht nach der Strafprozessordnung, sondern zu präventiven Zwecken, gestützt auf § 15a Abs. 5 Satz 5 HSOG, erhoben wurden, ist dabei nicht ohne Weiteres zu erkennen. In der mündlichen Verhandlung wurde zwar seitens des Hessischen Ministeriums des Innern und für Sport erklärt, Verkehrsdaten würden nur im Fall des § 25a Abs. 1 Alt. 2 HSOG, also zur Abwehr von Gefahren, nicht jedoch zur vorbeugenden Bekämpfung von Straftaten in die Datenanalyse einbezogen. Insoweit erscheint die verwertbare Menge von Verkehrsdaten für die hier allein zu beurteilende Datenanalyse nach § 25a Abs. 1 Alt. 1 HSOG jedenfalls praktisch begrenzt. Auch diese Begrenzung müsste jedoch hinreichend normenklar und transparent geregelt werden, zumal sie offenbar nicht über eine Datenkennzeichnung gesichert ist, die derzeit nicht erfolgt (oben Rn. 139). Soweit der Gesetzgeber die technisch-organisatorische Umsetzung der Ausnahme von Verkehrsdaten aus der Datenanalyse nicht selbst regeln kann, muss er die Verwaltung zur näheren Regelung der technischen Einzelheiten und deren Veröffentlichung verpflichten, wenn er das Eingriffsgewicht der automatisierten Datenanalyse auf diese Weise senken will.

(β) Vergleichbares gilt für die Einbeziehung von anderen Daten aus besonders schweren Eingriffen. Seitens des Hessischen Ministeriums des Innern und für Sport wurde in der mündlichen Verhandlung erklärt, auch diese Daten würden (wohl ebenfalls wegen § 479 Abs. 2 Satz 2 StPO) nur im Fall des § 25a Abs. 1 Alt. 2 HSOG, also zur Abwehr einer Gefahr, nicht aber zur vorbeugenden Verhütung von Straftaten in die Datenanalyse einbezogen. Demnach wären die für die Datenanalyse zur vorbeugenden Bekämpfung von Straftaten verwertbaren Daten auch insoweit jedenfalls praktisch begrenzt. 143

Allerdings ist insbesondere offen geblieben, wie es in der polizeilichen Praxis gelingen kann, Daten aus schweren Eingriffen bei der Erfassung von Neueingängen in dem automatisiert in die Analyseplattform eingebundenen Vorgangsbearbeitungssystem zuverlässig zu identifizieren und vor der automatisierten Datenanalyse auszusondern, obwohl eine Kennzeichnung im Vorgangsbearbeitungssystem nach allen hierzu in der mündlichen Verhandlung vorgetragenen Einschätzungen derzeit nicht erfolgt und auch gar nicht möglich ist. Bei den Daten der Vorgangsbearbeitung dürfte eine Aussonderung bestimmter Daten derzeit schon deshalb praktisch nicht erfolgen, weil der Zugriff auf die Daten der Vorgangsverwaltung im Rahmen einer automatisierten Anwendung nach § 25a HSOG gerade ermöglicht werden sollte, um sicherzustellen, dass auch Zugriff auf Daten besteht, die aufgrund ihrer Aktualität noch keinen Eingang in weitere polizeiliche Systeme gefunden haben (vgl. HessLTDrucks 19/6502, S. 40 f.); Aussonderungsschritte, in denen Daten aus schweren Eingriffen aus der Datenanalyse herausgehalten werden könnten, sind der Analyse also nicht vor- 144

geschaltet (vgl. auch Bäuerle, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, 27. Edition, Stand: 1. Oktober 2022, § 20 HSOG, Rn. 153).

Wiederum fehlen jedenfalls Vorschriften, die klar regeln, dass Daten aus besonders schweren Eingriffen vor der Durchführung einer Datenanalyse ausgesondert werden müssen und die die technisch-organisatorische Umsetzung dieses Aussonderungsgebots sicherstellen. Auch insoweit ist das Eingriffsgewicht der Datenanalyse daher nicht hinreichend zuverlässig reduziert. 145

(2) Spezifisch verstärkt wird das Eingriffsgewicht durch die nach den angegriffenen Regelungen möglichen Methoden der Datenverarbeitung. Dem Wortlaut nach lassen § 25a HSOG und § 49 HmbPolDVG sehr weitreichende Methoden der automatisierten Datenanalyse und -auswertung zu. Der Gesetzgeber hat nicht eingegrenzt, welche Methoden der Analyse und Auswertung erlaubt sind. 146

(a) Die angegriffenen Vorschriften schließen auch komplexere Formen des Datenabgleichs nicht aus. Wenn § 25a HSOG und § 49 HmbPolDVG von der automatisierten Anwendung zur Datenanalyse oder zur Datenauswertung, also nicht etwa vom (automatisierten) Abgleich, sprechen, hebt sich das bereits gesetzessystematisch vom einfachen Abgleich (s. § 25 HSOG, § 48 Abs. 1 HmbPolDVG) ab. § 25a HSOG und § 49 HmbPolDVG ermöglichen demgegenüber ein „Data-Mining“ (vgl. BVerfGE 156, 11 <40 Rn. 74>) bis hin zur Verwendung selbstlernender Systeme (KI). Dabei sind insbesondere auch offene Suchvorgänge zulässig (vgl. Rn. 93 ff.). Die Datenanalyse oder -auswertung darf darauf zielen, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, aus denen dann, möglicherweise auch mit Hilfe weiterer automatisierter Anwendungen, weitere Schlüsse gezogen werden. Die Vorschriften schließen auch bezüglich der erzielbaren Suchergebnisse nichts aus (vgl. Rn. 96 ff.); nach dem Wortlaut könnte das Suchergebnis in maschinellen Sachverhaltsbewertungen bestehen – bis hin zu Gefährlichkeitsaussagen über Personen im Sinne eines „predictive policing“. Es könnten also mittels Datenanalyse oder -auswertung neue persönlichkeitsrelevante Informationen erzeugt werden, auf die ansonsten kein Zugriff bestünde (vgl. Bäuerle, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, 27. Edition, Stand: 1. Oktober 2022, § 25a HSOG, Rn. 21). Diese potenzielle Weite erzielbaren neuen Wissens wird auch nicht durch eingriffsmildernde Regelungen zu dessen Verwendung flankiert. 147

(b) In Hamburg hat der Gesetzgeber den Versuch unternommen, so weitgehende Anwendungen auszuschließen, indem er anstelle des Wortes „Datenanalyse“ das Wort „Datenauswertung“ verwendet hat (Rn. 14). Jedoch hat sich auch im Hamburgischen Gesetz die Vorstellung, nur begrenzte Anwendungen zulassen zu wollen, im Wortlaut nicht maßgeblich niedergeschlagen. Eine verfassungsrechtlich ausreichende Klarstellung, dass durch die automatisierte Anwendung lediglich mittels bestimmter Suchkriterien Übereinstimmungen ausgewiesen werden, nicht jedoch die polizeiliche Aus- und Bewertung der Daten ersetzt werden sollten, ist mit der Wortlautumstellung von „Datenanalyse“ zu „Datenauswertung“ nicht gelungen. Ein 148

maßgeblicher Unterschied zwischen den Wörtern Datenanalyse und Datenauswertung ist nicht zu erkennen. In § 49 Abs. 2 HmbPolDVG wird zudem weiterhin auf Verarbeitungsziele abgestellt, für deren Erreichung Prozesse des „Data-Mining“ eingesetzt werden müssten (vgl. dazu auch BVerfGE 156, 11 <40 Rn. 74>).

(c) Die hier angegriffenen Befugnisse sind auch nicht dadurch verfassungsrechtlich relevant eingegrenzt, dass Techniken einer unbegrenzten Datenauswertung aktuell nicht zur Verfügung stünden. Ob dem so ist, muss hier nicht aufgeklärt werden. Denn auch wenn eine Norm Funktionsweiterungen erst infolge weiterer technischer Entwicklungen zulässt, richten sich die verfassungsrechtlichen Anforderungen grundsätzlich nach diesen weiteren Funktionen. Für das Eingriffsgewicht einer Norm sind auch nicht die bloße Vorstellung des Gesetzgebers von der begrenzten Reichweite einer Befugnis oder der Wille der Verwaltung, von den rechtlichen Möglichkeiten einer Befugnis nicht umfassend Gebrauch zu machen, maßgeblich. Das Gewicht ist vielmehr nach den rechtlich geschaffenen Eingriffsmöglichkeiten zu beurteilen. Wollte der Gesetzgeber das Eingriffsgewicht nachhaltig begrenzen, müsste er dies normenklar im Wortlaut der Regelung niederlegen (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 325 f.). 149

bb) Die Gesetzgeber in Hessen und in Hamburg haben die Befugnis zur automatisierten Datenanalyse oder -auswertung in § 25a HSOG und in § 49 HmbPolDVG aktuell also kaum eingegrenzt. Sie gestatten der Polizei damit Grundrechtseingriffe, die sehr schwer wiegen können. Die Befugnisse lassen die automatisierte Verarbeitung unbegrenzter Datenbestände mittels rechtlich unbegrenzter Methoden zu. In ihrer daten- und methodenoffenen Unbegrenztheit erlauben die Regelungen der Polizei, mit einem Klick umfassende Profile von Personen, Gruppen und Milieus zu erstellen und auch zahlreiche rechtlich unbeteiligte Personen weiteren polizeilichen Maßnahmen zu unterziehen, die in irgendeinem Zusammenhang Daten hinterlassen haben, deren automatisierte Auswertung die Polizei auf die falsche Spur zu ihnen gebracht hat. 150

Es gelten daher dieselben verfassungsrechtlichen Anforderungen, wie sie auch an andere tief in die Privatsphäre eingreifende Überwachungsmaßnahmen der Gefahrenabwehrbehörden gestellt werden. Die allgemeine Eingriffsschwelle für heimliche Überwachungsmaßnahmen der Gefahrenabwehrbehörden ist das Erfordernis einer konkretisierten Gefahr (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 248 m.w.N.; dazu im Einzelnen BVerfGE 141, 220 <272 f. Rn. 112>; 154, 152 <268 Rn. 219> und oben Rn. 106) für besonders gewichtige Rechtsgüter (vgl. BVerfGE 141, 220 <270 Rn. 108> und oben Rn. 105). Wenn demgegenüber in der Praxis, wie insbesondere in der mündlichen Verhandlung ausführlich dargelegt wurde, die rechtlichen Möglichkeiten der Befugnis bei weitem nicht ausgeschöpft werden, nicht ausgeschöpft werden sollen und angesichts des aktuellen Stands der Technik derzeit auch nicht voll ausgeschöpft werden könnten, ändert dies an den verfassungsrechtlichen Anforderungen nichts. 151

III.

§ 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG genügen danach nicht den Anforderungen der Verhältnismäßigkeit im engeren Sinne, weil sie keine hinreichende Eingriffsschwelle enthalten. Die Weiterverarbeitung mittels einer automatisierten Datenanalyse oder -auswertung ist gemäß § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG in begründeten Einzelfällen zulässig, wenn dies zur vorbeugenden Bekämpfung von in § 100a Abs. 2 StPO genannten Straftaten erforderlich ist. Die „vorbeugende Bekämpfung von Straftaten“ ist in § 1 Abs. 1 Satz 2 Nr. 1 HmbPolDVG und in § 1 Abs. 4 HSOG definiert als Verhütung von Straftaten beziehungsweise zu erwartenden Straftaten (1) und Vorsorge für die Verfolgung künftiger Straftaten (2). In beiden Alternativen bleibt der Eingriffsanlass weit hinter der wegen des Eingriffsgewichts verfassungsrechtlich gebotenen Schwelle einer konkretisierten Gefahr zurück. Über die Frage, ob ausreichend gewichtige Rechtsgüter normiert sind, ist hier nicht zu entscheiden (oben Rn. 48). 152

1. Soweit § 25a Abs. 1 Alt. 1 in Verbindung mit § 1 Abs. 4 HSOG und § 49 Abs. 1 Alt. 1 in Verbindung mit § 1 Abs. 1 Satz 2 Nr. 1 HmbPolDVG zur Datenanalyse oder -auswertung zwecks Verhütung der in § 100a Abs. 2 StPO genannten Straftaten ermächtigen, ist der Eingriffsanlass angesichts des beschriebenen Eingriffsgewichts unverhältnismäßig weit und damit verfassungswidrig geregelt. 153

a) Indem die Regelungen eine automatisierte Datenanalyse oder -auswertung allgemein zur Verhütung schwerer Straftaten erlauben, fehlt eine hinreichend eingrenzende Konkretisierung des Eingriffsanlasses und ist das Erfordernis einer wenigstens konkretisierten Gefahr nicht erfüllt (vgl. auch BVerfGE 141, 220 <336 Rn. 313>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 375). Die hessische Regelung enthält zwar den Zusatz der „zu erwartenden“ Straftat. Dennoch bleibt auch sie weit hinter dem Erfordernis einer konkretisierten Gefahr zurück. Eine Erweiterung der polizeilichen Aufgabe in zeitlicher und sachlicher Hinsicht gegenüber der in § 1 Abs. 1 HSOG genannten Gefahrenabwehr, „weg von der konkreten Tat“, ist auch hier gerade der Sinn der Aufgabenbeschreibung in § 1 Abs. 4 HSOG (vgl. Mühl/Fischer, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, 27. Edition, Stand: 1. Oktober 2022, § 1 HSOG, Rn. 128). 154

b) Auch die weitere Maßgabe beider Regelungen, es müsse ein begründeter „Einzelfall“ vorliegen, enthält hier kaum nähere inhaltliche Festlegungen. 155

aa) Das Einzelfallerfordernis ist schon nicht hinreichend bestimmt. So bestehen Zweifel, worauf sich das Tatbestandsmerkmal des Einzelfalls bezieht. Der Hessische Minister des Innern und für Sport hat – damals nach § 25a Abs. 3 HSOG befragt – dargelegt, nicht das einzelne Ermittlungsverfahren sei als Einzelfall anzusehen, sondern ein Einzelfall im Sinne von § 25a HSOG sei ein „Vorgang bzw. ein Projekt, das an ein Ermittlungsverfahren anknüpft“ (vgl. HessLTDrucks 20/660, S. 1 f.). Weder diese besonders weite Inbezugnahme eines „Projekts“ noch die etwas engere Anknüpfung an einzelne Ermittlungsverfahren würden der hier geltenden verfassungs- 156

rechtlichen Maßgabe genügen, dass jede einzelne Weiterverwendung eines jeden Datums von Bedeutung für die Abwehr einer wenigstens konkretisierten Gefahr sein muss (vgl. BVerfGE 150, 244 <286 f. Rn. 108>). In der mündlichen Verhandlung hat das Hessische Ministerium des Innern und für Sport allerdings dargelegt, dass die Voraussetzungen des § 25a HSOG bei jeder einzelnen Datenanalyse geprüft würden. Dies müsste dann aber auch normenklar geregelt werden.

bb) In der Sache bleibt die Voraussetzung des begründeten „Einzelfalls“ aber in jedem Fall hinter der hier verfassungsrechtlich gebotenen Schwelle einer wenigstens konkretisierten Gefahr zurück. 157

(1) Zwar schließt das Einzelfallerfordernis, wenn es auf jede einzelne Datenanalyse oder -auswertung angewendet wird, aus, dass ins Blaue hinein (vgl. dazu BVerfGE 130, 151 <205>) automatisierte Datenanalysen oder -auswertungen gestartet und so durch massenhafte Datenverarbeitung sachliche Anhaltspunkte für eine künftige Begehung von Straftaten überhaupt erst generiert werden. Das Einzelfallerfordernis dürfte daher etwa der Voraussetzung eines Spurenansatzes entsprechen (vgl. dazu BVerfGE 141, 220 <325 f. Rn. 281>). Allein daraus, dass Daten und Datenbestände durch Einzelakt einbezogen werden und für die konkrete Verhütungsmaßnahme erforderlich sein müssen, mag so praktisch bereits ein gewisser begrenzender Effekt folgen (vgl. BVerfGE 130, 151 <205>). Von einer wenigstens konkretisierten Gefahr ist dies jedoch noch weit entfernt. 158

(2) In der mündlichen Verhandlung wurde allerdings ein engeres Konzept beschrieben, nach dem die Voraussetzung des „Einzelfalls“ in der hessischen Polizeipraxis verstanden und angewendet werde. Es werde durchgehend an eine bereits begangene Straftat oder wenigstens den durch Tatsachen belegten Verdacht einer bereits begangenen Straftat angeknüpft und daraus eine Prognose für die Zukunft hergeleitet: Zum einen müsse für die Vergangenheit davon ausgegangen werden können, dass bereits eine Straftat nach § 100a Abs. 2 StPO begangen wurde. Zum anderen müsse aufgrund dieser Situation für die Zukunft mit weiteren, gleichgelagerten Straftaten zu rechnen sein. 159

(a) Durch die Verengung auf Konstellationen, in denen eine hinreichende Tatsachengrundlage für die Annahme besteht, dass eine Straftat bereits begangen wurde, wird der Anwendungsbereich von § 25a Abs. 1 Alt. 1 HSOG eingeschränkt. Zwar dürfte die Polizei die in § 25a Abs. 1 HSOG präventiv formulierte Datenanalysebefugnis – ungeachtet der Frage einer Gesetzgebungskompetenz – schon mangels gesetzlicher Grundlage nicht als Strafverfolgungsinstrument nutzen. Wenn die Prüfung eines hinreichenden Tatverdachts jedoch nur der Feststellung dient, ob sich daraus Anhaltspunkte für die Begehung künftiger gleichgelagerter Straftaten ergeben, könnte dies den präventiven Charakter der Datenanalyse wahren. Praktisch kommt die Datenanalyse dann insbesondere hinsichtlich solcher Straftaten in Betracht, die regelmäßig in Serie begangen werden, so dass aus der Begehung einer Straftat unter bestimmten Umständen auf die Begehung weiterer Straftaten geschlossen werden 160

kann. Dies engt den Anwendungsbereich von § 25a Abs. 1 Alt. 1 HSOG weiter ein.

(b) Würde allerdings aus einer abstrakten Annahme, dass bestimmte Straftaten häufig in Serie begangen werden, generell darauf geschlossen, dass eine künftige Begehung solcher Straftaten drohe, bliebe der Eingrenzungseffekt geringer. Vielmehr stellt erst eine nähere Betrachtung, ob die konkreten Umstände der einzelnen (vermutlich) begangenen Straftat erwarten lassen, dass weitere entsprechende Taten begangen werden, einen tatsächlichen Einzelfallbezug her. Nach Darstellungen in der mündlichen Verhandlung werden in der hessischen Praxis die den Straftatverdacht begründenden konkreten Umstände näher betrachtet und wird daraus aufgrund kriminalistischer Erfahrungssätze eine Prognose zur Erwartbarkeit weiterer Straftaten abgeleitet; eine solche Handhabung der Norm hätte eingrenzende Wirkung. Zugleich wurde aber erklärt, es erfolge eine generalisierende Identifikation von Kriminalitätsfeldern, in denen grundsätzlich mit weiteren Straftaten gerechnet und daher in jedem Einzelfall davon ausgegangen werden müsse, dass weitere Straftaten drohen; dies schwächt den eingrenzenden Effekt wieder ab. Weil keine öffentlich zugängliche Dokumentation der hessischen Anwendungspraxis vorliegt, kann dies hier nicht näher beurteilt werden. 161

(c) Der eingrenzende Effekt ist zudem verringert, wenn im Einzelfall nicht auch näher geprüft wird, ob die einzelnen in die Analyse eingestellten Daten geeignet sind, zur Verhütung der möglicherweise bevorstehenden Serientat beizutragen. Ohnehin genügt eine Maßnahme der Datenverarbeitung Verhältnismäßigkeitsanforderungen grundsätzlich nur, wenn die einzubeziehenden personenbezogenen Daten auf solche beschränkt werden, die für den jeweiligen Zweck der Maßnahme Bedeutung haben können (vgl. BVerfGE 150, 244 <286 f. Rn. 108 f.>). Denn wenn eine Datenanalyse oder -auswertung zur Verhütung bestimmter Straftaten erlaubt wird, müssen auch die einzelnen Analyse- und Abgleichvorgänge von diesem Zweck her ihre Begrenzung finden. Sollen Datenbestände in die Datenanalyse oder -auswertung einbezogen werden, die mit diesem Zweck nichts zu tun haben, so bedürfte dies eines eigenen tragfähigen Grunds. Ohne einen solchen Grund ist eine Maßnahme, die Datenbestände einbezieht, die von vornherein zu dem Zweck der konkreten Datenanalyse oder -auswertung nicht beitragen können, unverhältnismäßig (vgl. BVerfGE 150, 244 <288 Rn. 111>). 162

In der hessischen Praxis scheint zwar eine Einzelfallprüfung der Eignung der vorhandenen Daten konzeptionell vorgesehen zu sein. Die Eignung aller in der Analyseplattform bereitstehenden Daten, einschließlich der Daten aus der Vorgangsbearbeitung, wird aber nach Darstellung des Hessischen Ministeriums des Innern und für Sport in der mündlichen Verhandlung bereits daraus gefolgert, dass diese Daten generell geeignet seien, zum Erkenntnisziel des Einzelfalls beizutragen. Eine nähere Prüfung der konkreten Eignung scheint insoweit also nicht vorgenommen zu werden. Tatsächlich wäre eine konkrete Eignungsprüfung für jedes Datum angesichts der in Hessen wegen der Einbeziehung der Daten aus der Vorgangsverwaltung sehr umfangreichen Datenmengen praktisch auch schwer vorstellbar. Umso wichtiger wäre 163

auch hier eine normenklare, durch transparente technisch-organisatorische Maßgaben hinterlegte Regelung dazu, welche Daten überhaupt in die einzelne Datenanalyse einbezogen werden können.

(d) Ungeachtet der näheren Ausgestaltung der hessischen Anwendungspraxis sind die verfassungsrechtlichen Anforderungen derzeit aber schon deshalb nicht erfüllt, weil das Konzept der hessischen Praxis von vornherein nicht auf die Identifizierung einer wenigstens konkretisierten Gefahr und der zu deren Abwehr geeigneten Daten zielt. Das ist aber wegen der daten- und methodenoffenen Ausgestaltung der Befugnis in § 25a HSOG und § 49 HmbPolDVG erforderlich. 164

Würde die Befugnis hingegen hinsichtlich Art und Umfang der Daten und zulässiger Verarbeitungsmethoden enger gefasst und die potenzielle Eingriffsintensität dadurch so weit gesenkt, dass eine niedrigere Eingriffsschwelle verfassungsrechtlich genügen würde (Rn. 75 ff., 107), könnte das aktuelle Konzept der hessischen Praxis Ausgangspunkt einer verfassungskonformen Ausgestaltung der Eingriffsvoraussetzungen sein. Im Einzelnen kann und muss dies hier nicht entschieden werden. Ein solches Konzept müsste dann jedenfalls unter Wahrung der Anforderungen des Gesetzesvorbehalts, der Normenklarheit und des Bestimmtheitsgebots näher geregelt werden. Derzeit findet sich in § 25a HSOG kein Anhaltspunkt für das Konzept der hessischen Polizei. 165

cc) In anderen sicherheitsrechtlichen Konstellationen hat das Bundesverfassungsgericht zwar, wie beide Landesregierungen geltend machen, ein Einzelfallerfordernis genügen lassen. Unproblematisch kann es zur weiteren Qualifizierung einer durch andere Merkmale bereits näher umschriebenen Schwelle dienen (vgl. BVerfGE 141, 220 <272 Rn. 112>). Insbesondere dann, wenn die Befugnis voraussetzt, dass eine Maßnahme im Einzelfall zur Abwehr einer Gefahr erforderlich sein muss, kann dies eine nähere Spezifizierung des Gefahrerfordernisses ersetzen und als hinreichend bestimmte Umschreibung des Erfordernisses einer konkreten Gefahr gelten, wenn zu keinem besonders schweren Grundrechtseingriff ermächtigt wird (vgl. BVerfGE 130, 151 <205>; 155, 119 <192 Rn. 158>). Bei nachrichtendienstlichen Eingriffen, die immer dem Schutz besonders gewichtiger Rechtsgüter dienen müssen, kann das Einzelfallerfordernis, wenn die Maßnahme für sich genommen nicht tief in die Privatsphäre eingreift, die eigentliche Eingriffsschwelle der Aufklärungsbedürftigkeit einer beobachtungsbedürftigen Aktion oder Bestrebung verfassungsrechtlich ausreichend qualifizieren (vgl. BVerfGE 130, 151 <206>; 155, 119 <189 Rn. 151>; 156, 11 <59 Rn. 126>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 206). All das trifft hier jedoch nicht zu. 166

Die hier angegriffenen Regelungen gleichen insoweit auch nicht § 6a Abs. 3 ATDG, der mit dem Grundgesetz vereinbar ist. Zwar spricht auch diese Ermächtigung zur erweiterten Datennutzung vom Einzelfall, sieht jedoch strengere Voraussetzungen vor. Danach darf eine beteiligte Behörde des Bundes zur Erfüllung ihrer gesetzlichen Aufgaben die in der Datei gespeicherten Datenarten erweitert nutzen, soweit dies im 167

Rahmen eines bestimmten einzelfallbezogenen Projekts für die Verhinderung von qualifizierten Straftaten des internationalen Terrorismus erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären, und Tatsachen die Annahme rechtfertigen, dass eine solche Straftat begangen werden soll. Dies ist mehrfach enger als § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG. Insbesondere muss die erweiterte Nutzung der Antiterrordatei erforderlich sein, „um weitere Zusammenhänge des Einzelfalls“ aufzuklären. Letzteres wird bei verfassungskonformer Auslegung von § 6a Abs. 3 ATDG so verstanden, dass eine weitere Nutzung der Datei erst zulässig ist, wenn die Behörde bereits ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennt oder erkennt, dass das individualisierte Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in absehbarer Zeit terroristische Straftaten begeht. Die erweiterte Nutzung setzt demnach eine solchermaßen konkretisierte Gefahr voraus, zu deren weiterer Aufklärung sie, was hinreichend klar erkennbar ist, dienen muss (BVerfGE 156, 11 <61 Rn. 130>). Diese eingrenzenden Tatbestandsvoraussetzungen enthalten § 25a HSOG und § 49 HmbPolDVG nicht.

c) Für das hamburgische Recht lässt sich die erforderliche Begrenzung der Befugnis aus § 49 Abs. 1 Alt. 1 HmbPolDVG auch nicht aus anderen Vorschriften des Gesetzes entnehmen. Zwar knüpft § 11 Abs. 1 Nr. 6 HmbPolDVG die Verarbeitung personenbezogener Daten, zu der die Datenauswertung nach § 49 HmbPolDVG gehört (vgl. § 2 Abs. 8 HmbPolDVG), zum Zweck der Straftatverhütung allgemein daran, dass tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird, und die Erhebung zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist. Es mag systematisch nicht ausgeschlossen sein, dies als stets geltende Mindestvoraussetzung der Verarbeitung personenbezogener Daten zum Zweck der Verhütung von Straftaten zu verstehen. Allerdings begreift der hamburgische Gesetzgeber § 49 HmbPolDVG als Spezialregelung, auf die das allgemeine Erfordernis des § 11 Abs. 1 Nr. 6 HmbPolDVG keine Anwendung finden soll. Ein von dieser, in der mündlichen Verhandlung bekräftigten, Auffassung abweichendes Verständnis wäre mit der zu respektierenden gesetzgeberischen Grundentscheidung nicht zu vereinbaren. 168

d) Die hier angesichts der konkreten Ausgestaltung der Datenanalyse oder -auswertung verfassungsrechtlich gebotene Begrenzung der Befugnis auf Fälle einer wenigstens konkretisierten Gefahr ist auch nicht dadurch erfolgt, dass die Datenanalyse oder -auswertung nur im „begründeten“ Einzelfall zugelassen ist. Selbst wenn bei engerer Ausgestaltung der Befugnis de lege ferenda eine niedrigere Eingriffsschwelle ausreichen würde, ist nicht ersichtlich, inwiefern das Tatbestandsmerkmal des „begründeten“ Einzelfalls die Reichweite der Befugnis reduzieren könnte. Insbesondere ist nicht erkennbar, dass hieraus weitere materielle Maßgaben folgen. In der mündlichen Verhandlung wurde seitens des Hessischen Ministeriums des Innern und für Sport erklärt, der Einzelfall müsse in dem Sinne begründet sein, dass die in zweifacher Richtung verdichtete Tatsachenbasis vorliegen müsse (oben Rn. 159); das geht 169

aber nicht über die in der hessischen Praxis bereits aus dem Einzelfallerfordernis abgeleiteten Anforderungen hinaus und findet im Übrigen in dem Wort „begründet“ ebenso wenig gesetzliche Stütze wie in dem Wort „Einzelfall“. Dargelegt wurde in der mündlichen Verhandlung auch, dass es nicht darum gehe, die Maßnahme mit einer Begründung zu versehen (zur Notwendigkeit Rn. 109). Auch ansonsten würden hieraus keine prozeduralen Anforderungen abgeleitet. Insgesamt ist danach nicht erkennbar, dass die Befugnis durch das Kriterium des „begründeten“ Einzelfalls in hinreichender Klarheit beschränkt wird.

e) § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG regeln auch deshalb keine hinreichende Eingriffsschwelle, weil über den Katalog des § 100a Abs. 2 StPO auch Gefährdungstatbestände erfasst sind. Eine Anknüpfung der Eingriffsschwelle an das Vorfeld von konkreten Rechtsgutsgefahren oder -verletzungen ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn zu diesem Zeitpunkt nur relativ diffuse Anhaltspunkte für mögliche Rechtsgutsbeeinträchtigungen bestehen (vgl. BVerfGE 141, 220 <273 Rn. 113> m.w.N.). Daher entspricht es nicht ohne Weiteres verfassungsrechtlichen Anforderungen, wenn die Ermächtigung zur Erhebung personenbezogener Daten als Eingriffsschwelle an die Gefahr der Begehung solcher Straftaten anknüpft, bei denen die Strafbarkeitsschwelle durch die Einbeziehung von Vorbereitungshandlungen in das Vorfeld von konkreten Rechtsgutsgefahren oder -verletzungen verlagert wird. Zwar kann auch mit der Verwirklichung eines Vorfeldtatbestands eine konkretisierte oder konkrete Gefahr für die jeweils geschützten Rechtsgüter einhergehen. Sicher ist dies jedoch nicht; allein aus der Gefahr der Verwirklichung eines Vorfeldtatbestands ergeben sich nicht notwendigerweise bereits solche Gefahren für Rechtsgüter. Gerade auf eine Gefahr für die geschützten Rechtsgüter kommt es aber an. Zwar ist dem Gesetzgeber verfassungsrechtlich nicht verwehrt, zur Bestimmung der Eingriffsvoraussetzungen auch an die Gefahr der Begehung von Vorfeldtatbeständen anzuknüpfen. Er muss dann aber eigens sicherstellen, dass in jedem Einzelfall eine konkrete oder konkretisierte Gefahr für die durch den Straftatbestand geschützten Rechtsgüter vorliegt. Knüpft der Gesetzgeber an die Begehung solcher Straftaten an, muss er also zusätzlich fordern, dass damit bereits eine konkretisierte oder konkrete Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt (vgl. BVerfG, Beschluss des Ersten Senats vom 28. September 2022 - 1 BvR 2354/13 -, Rn. 134; Beschluss des Ersten Senats vom 9. Dezember 2022 - 1 BvR 1345/21 -, Rn. 92). Daran fehlt es hier. 170

2. Die vorbeugende Bekämpfung von Straftaten im Sinne von § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG umfasst nach der Definition in § 1 Abs. 4 HSOG und § 1 Abs. 1 Satz 2 Nr. 1 HmbPolDVG nicht nur die Verhütung von Straftaten, sondern auch die Vorsorge zur Verfolgung künftiger Straftaten. Polizeiliche Datenbestände sollen im Wege der automatischen Datenauswertung genutzt werden, um Erkenntnisse für die zukünftige Aufklärungsarbeit und Ermittlungsverfahren zu gewinnen (vgl. Mühl/Fischer, in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, 27. Edition, Stand: 1. Oktober 2022, § 1 HSOG, Rn. 132). Dass bereits eine 171

Sachlage gegeben sein müsste, bei der eine konkrete oder eine konkretisierte Gefahr besteht, ist dem nicht zu entnehmen. Damit fehlt es auch hier an jeder eingrenzenden Konkretisierung des Eingriffsanlasses (vgl. auch BVerfGE 141, 220 <336 Rn. 313>).

Der Deutung des Hamburgischen Senats, § 49 Abs. 1 HmbPolDVG weise unter Berücksichtigung des Merkmals „in begründeten Einzelfällen“ gar keinen Bezug zur Vorsorge für die Verfolgung künftiger Straftaten auf, kann angesichts der klaren Definition in § 1 Abs. 1 Satz 2 Nr. 1 HmbPolDVG nicht gefolgt werden. Die Strafverfolgungsvorsorge müsste vielmehr ausdrücklich ausgenommen werden. 172

D.

I.

Im Ergebnis sind § 25a Abs. 1 Alt. 1 HSOG und § 49 Abs. 1 Alt. 1 HmbPolDVG verfassungswidrig. Sie verstoßen gegen das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG in seiner Ausprägung als informationelle Selbstbestimmung, weil sie keine dem mit diesen Maßnahmen der Datenanalyse und -auswertung verbundenen Eingriffsgewicht angemessene Eingriffsschwelle vorsehen. Im Übrigen haben die Verfassungsbeschwerden keinen Erfolg, weil hinsichtlich der weiteren Beanstandungen die Möglichkeit einer Grundrechtsverletzung nicht hinreichend dargelegt wurde. 173

II.

1. Die Feststellung der Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu deren Nichtigkeit. Allerdings kann sich das Bundesverfassungsgericht, wie sich aus § 31 Abs. 2 Sätze 2 und 3 BVerfGG ergibt, auch darauf beschränken, eine verfassungswidrige Norm nur für mit der Verfassung unvereinbar zu erklären. Es verbleibt dann bei einer bloßen Beanstandung der Verfassungswidrigkeit ohne den Ausspruch der Nichtigkeit. Die Unvereinbarkeitserklärung kann das Bundesverfassungsgericht dabei zugleich mit der Anordnung einer befristeten Fortgeltung der verfassungswidrigen Regelung verbinden. Dies kommt in Betracht, wenn die sofortige Ungültigkeit der zu beanstandenden Norm dem Schutz überragender Güter des Gemeinwohls die Grundlage entziehen würde und eine Abwägung mit den betroffenen Grundrechten ergibt, dass der Eingriff für eine Übergangszeit hinzunehmen ist. Für die Übergangszeit kann das Bundesverfassungsgericht vorläufige Anordnungen treffen, um die Befugnisse der Behörden bis zur Herstellung eines verfassungsmäßigen Zustands durch den Gesetzgeber auf das zu reduzieren, was nach Maßgabe dieser Abwägung geboten ist (BVerfGE 141, 220 <351 Rn. 355> m.w.N.; stRspr). 174

2. Danach ist § 25a Abs. 1 Alt. 1 HSOG nur für mit der Verfassung unvereinbar zu erklären. Die Unvereinbarkeitserklärung ist mit der Anordnung ihrer vorübergehenden Fortgeltung bis zu einer Neuregelung, längstens jedoch bis zum Ablauf des 30. September 2023 zu verbinden. Anschließend ist die Norm nicht mehr anwendbar. 175

Angesichts der Bedeutung, die der Gesetzgeber der Befugnis für die staatliche Aufgabenwahrnehmung beimessen darf und wegen ihrer Bedeutung für die Praxis vorbeugender Straftatenbekämpfung durch die hessische Polizei, die die Befugnis hierfür regelmäßig nutzt, dabei bislang aber – insoweit grundrechtsschonend – von den besonders weitgehenden Nutzungsmöglichkeiten nicht Gebrauch macht, ist eine befristete Fortgeltung eher hinzunehmen als eine Nichtigerklärung.

Die befristete Anordnung der Fortgeltung bedarf mit Blick auf die betroffenen Grundrechte jedoch einschränkender Maßgaben, die eine Neuregelung durch den Gesetzgeber aber nicht präjudizieren. Unter Zugrundelegung des in der hessischen Praxis gewählten Konzepts wird angeordnet, dass von der Befugnis des § 25a Abs. 1 Alt. 1 HSOG nur Gebrauch gemacht werden darf, wenn bestimmte, genügend konkretisierte Tatsachen den Verdacht begründen (vgl. BVerfGE 154, 152 <268 Rn. 219>; 156, 11 <56 Rn. 120>), dass eine besonders schwere Straftat im Sinne von § 100b Abs. 2 StPO begangen wurde und aufgrund der konkreten Umstände eines solchen im Einzelfall bestehenden Tatverdachts für die Zukunft mit weiteren, gleichgelagerten Straftaten zu rechnen ist, die Leib, Leben oder den Bestand oder die Sicherheit des Bundes oder eines Landes gefährden, wenn das Vorliegen dieser Voraussetzungen und die konkrete Eignung der verwendeten Daten nach § 25a Abs. 1 Alt. 1 HSOG zur Verhütung der zu erwartenden Straftat durch eigenständig auszuformulierende Erläuterung begründet wird und wenn sichergestellt ist, dass keine Informationen in die Datenanalyse einbezogen werden, die aus Wohnraumüberwachung, Online-Durchsuchung, Telekommunikationsüberwachung, Verkehrsdatenabfrage, länger andauernder Observation, unter Einsatz von verdeckt ermittelnden Personen oder Vertrauenspersonen oder aus vergleichbar schwerwiegenden Eingriffen in die informationelle Selbstbestimmung gewonnen wurden. 176

3. Hingegen ist § 49 Abs. 1 Alt. 1 HmbPolDVG für verfassungswidrig und nichtig zu erklären, weil keine Umstände ersichtlich sind, die eine befristete Fortgeltungsanordnung erforderten und rechtfertigten. Es wurde schon nicht dargelegt, dass beabsichtigt wäre, für eine wirksame vorbeugende Bekämpfung von Straftaten kurz- oder mittelfristig von der in § 49 Abs. 1 Alt. 1 HmbPolDVG enthaltenen Ermächtigung Gebrauch zu machen. 177

III.

Die Auslagenerstattung beruht auf § 34a Abs. 2 und 3 BVerfGG. 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_1bvr154719.html

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